Research Insights

—

COVID-19 cyberwar: How to protect your business

Attacks are escalating amid the pandemic—Our step-by-step security guide for action now

IBM **Institute for Business Value**

IBM

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

By Wendi Whitmore
and Gerald Parham

Key takeaways

COVID-19 and cybercrime

While the world struggles with the impacts of COVID-19, cybercriminals see it as an opportunity. Since February, IBM X-Force has observed a 4,300 percent increase in coronavirus-themed spam. *Action: Run simulations that model the most likely threat to mitigate any vulnerabilities now.*

Improvising amid chaos

Organizations that were insufficiently prepared in normal times have been caught completely off guard. In fact, 76 percent of organizations don't have an incident response plan applied consistently across the organization, according to a 2019 report.[1] *Action: Create or update a Cybersecurity Incident Response Plan (CSIRP).*

Managing through disruption

During times of crisis, business continuity planning becomes a major strategic asset. Even organizations that are unprepared can take steps to mitigate the impacts and use the experience for future crisis planning. *Action: Observe, orient, decide, and act in rapid cycles.*

Learning from extreme events

In recent weeks, cybersecurity threats have escalated, as bad actors take advantage of the COVID-19 pandemic. While organizations worry about newly pressing concerns—workforce well-being, finance availability, and the resiliency of operations and supply chains—cybersecurity focus is being overshadowed and risks are rising.

The tendency toward ad hoc decision making during crises only accelerates the opportunity to exfiltrate data or compromise business operations. The potential impacts are more dangerous, too. A distributed denial-of-service (DDoS) attack, for instance, can be far more damaging in an operational environment that is already strained for capacity than one launched when additional capacity is readily available.

In this report, we identify key steps security leaders can take now to manage discrete, high-impact events that may arise in this environment and to prepare for additional unforeseen scenarios. Every cybersecurity crisis has a three-part lifecycle:

- Planning and detection
- In-the-moment response and remediation
- Recovery.

The first step is for leaders to identify where they are in that lifecycle and prioritize their actions accordingly. We have created recommended actions for each phase as a guide. In particular, the current pandemic environment demands increased attention to response and remediation. Drawing on lessons learned from incident response drills in security operations centers (SOCs) and cyber ranges (virtual environments for testing security capabilities), we have found that highly resilient organizations do three things well: organize and deploy resources, communicate regularly, and coordinate responses.

50+

unique malware distributed in various COVID-19-themed campaigns[2]

1 in 4

organizations don't have an incident response plan[3]

#1

The combined effect of an incident response (IR) team and IR plan testing produces greater cost savings than any other security remediation process[4]

COVID-19's impact on the cybersecurity landscape

During 2020, business has changed radically for nearly every organization around the globe. As the number of COVID-19 cases grows and the rate of transmission accelerates in some areas and abates in others, the operations landscape evolves daily–sometimes hourly. The magnitude of impact is unprecedented.

Opportunistic threat actors

Since February when the outbreak went global, IBM X-Force has observed a 4,300 percent increase in coronavirus-themed spam. Cybercriminals are using the coronavirus outbreak to drive their business, with virus-themed sales of malware assets on the dark web and even virus-related discount codes.[5] They are also rapidly creating domains: COVID-19-related domains are 50 percent more likely to be malicious than other domains registered during the same time period.[6]

Numerous phishing scams have emerged. For example, IBM's X-Force Exchange is tracking a spam email that takes advantage of small business owners hoping to secure loans from the US Small Business Administration. Instead of providing help, an attachment installs a Remote Access Trojan (RAT). Another high-volume spam campaign threatens to infect recipients and their families with COVID-19 if they do not pay a ransom in bitcoin.[7]

A number of other scams imply association with legitimate health organizations. One email phishing attack purports being from the World Health Organization (WHO) director-general. Attached to the email are documents that install an Agent Tesla malware variant that acts as a keylogger and info-stealer.[8] A similar attack uses the US Centers for Disease Control and Prevention (CDC) as a lure.[9] The IBM X-Force COVID-19 security bulletins, which consolidate a collection of threat actors and COVID-19 exploits, identify hundreds of examples.[10]

Reports suggest nation-state actors could be using the pandemic to make forays into US public health agencies, notably the US Department of Health and Human Services.[11] As Ben Sasse, a member of the US Senate Intelligence Committee, observed, "Here's the reality of 21st century conflict: cyberattacks are massive weapons to kick opponents when they're down."[12]

Insight: Cybercrime damages public confidence

Cybercrime is built on threat actors' abilities to exploit fear, anxiety, and uncertainty, sentiments magnified during a pandemic. Compounding personal concerns, livelihoods of individuals and businesses are disrupted in unpredictable ways. As a World Economic Forum bulletin noted, society's increased reliance on digital infrastructure raises the cost of failure.[13] This public health pandemic imposes both social and economic costs, affecting individuals in unique and profound ways. High-value assets (HVAs) are particularly vulnerable to attack. Defined by the US Cybersecurity and Infrastructure Security Agency (CISA) as "information or systems so critical that their loss or corruption would seriously affect an organization's ability to perform its mission or conduct business," HVAs are especially enticing for cybercriminals looking to damage public confidence in an organization.[14]

The new risks of remote work

The rapid shift to remote work has also opened new loopholes for cybercriminals to exploit. According to *The New York Times*, as of the first week of April 2020, 316 million people in the US were being urged to stay home.[15] The global figures are orders of magnitude higher. India's shelter-in-place guidelines, for example, extend restrictions to 1.3 billion people.[16]

Many of those staying home are also working from home. Yet, many displaced workers lack the secure equipment or protocols that enable digital safety. With newly remote employees accessing corporate networks via personal devices, hackers are probing Wi-Fi configurations and VPN connections for security vulnerabilities. And as people congregate on cloud-based productivity platforms—both for work and personal reasons—malicious actors are launching schemes to exploit the situation, including hacking into and disrupting live meetings.[17]

Employees aren't the only ones who are unprepared—so are organizations. In a recent online poll by Threatpost, 70 percent of respondents said enabling remote working is fairly new for their organizations. And 40 percent reported seeing increased cyberattacks as they enable remote working.[18] As US Senator Mark Warner wrote in an email, "As the federal government prepares for what is likely to be an unprecedented experiment in telework, it's also expanding opportunities for malicious actors to attack and potentially disrupt vital government services."[19]

The potential for continued disruption during this pandemic is high and requires crisis response leaders to maintain constant vigilance and organizational agility.

Highly resilient organizations marshal resources, communicate efficiently, and coordinate responses.

The importance of making quick decisions

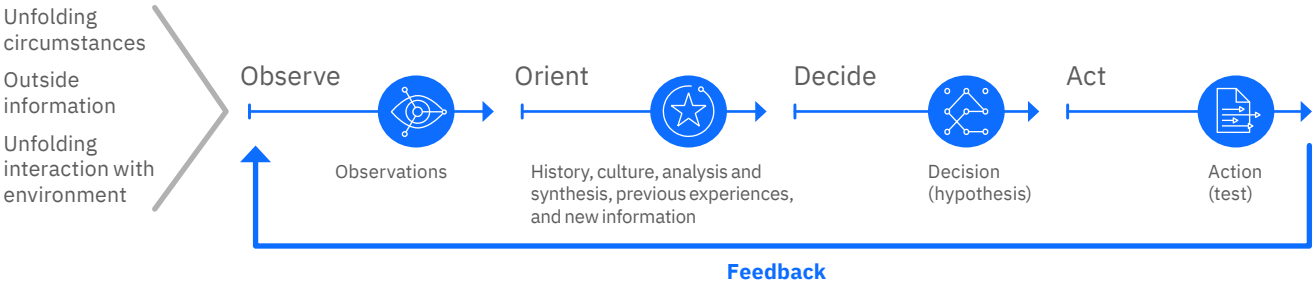
During a crisis, executives and members of security teams need to filter available information to quickly make optimal decisions. Borrowing principles originally developed by military strategists, organizations benefit from incorporating tactical operations techniques such as "observe, orient, decide, and act," also known as the OODA loop.[20]

The OODA loop encourages iteration (see Figure 1). If you can go through it faster than whatever you're remediating, you gain an advantage. By accelerating response, you can harmonize efforts with the broader team. No decision has to be final. Making small mistakes is often better than taking no action at all.

—

Figure 1

Observe, Orient, Decide, Act (OODA) Loop



Source: "OODA loop." Wikipedia, accessed April 1, 2020. https://en.wikipedia.org/wiki/OODA_loop

Creating an incident response plan

Most organizations are ill-equipped to handle a major cybersecurity incident, much less amid a global crisis like COVID-19. A recent study from the Ponemon Institute found that 76 percent of organizations don't have an incident response plan applied consistently across the organization. One in four organizations report not having any Cybersecurity Incident Response Plan (CSIRP) whatsoever.[21]

An effective CSIRP outlines governance and communications practices across teams (see "Insight: Anatomy of a CSIRP"). It also defines response models and details crisis response roles and responsibilities across the organization, such as strategy, technology, operations, and community and government relations. Any organization without a CSIRP in place should be racing to implement one. With breach notification laws and regulations getting stricter around the world even prior to the COVID-19 pandemic, business continuity planning is a long-term strategic capability that can prepare an organization for a host of unexpected contingencies.

But even if your organization has a CSIRP in place, there are steps you can take now to reinforce it for COVID-19's particular risks. Crisis management plans vary based on the nature and scope of the threat, the type and size of an organization, and variances in regulatory requirements related to disclosures, data privacy, and data locality. As organizations learn more, they can adapt the CSIRP and apply those lessons quickly.

Insight: Anatomy of a CSIRP

A Cybersecurity Incident Response Plan (CSIRP) typically includes the following information:

- How to qualify and classify a crisis event
- Roles and responsibilities of internal and external team members, including a hierarchical view that summarizes decision-making authority and escalations
- A crisis communications plan for communicating with internal and external stakeholders
- An inventory of the organization's HVAs and mission critical capabilities, along with the critical support services that enable these
- Regulatory and disclosure requirements related to the above
- An inventory of supplemental operations support capabilities like threat remediation services and threat intelligence sharing with community/computer emergency response/readiness teams (CERTs), federal law enforcement, or other groups.

Making small mistakes is often better than taking no action at all.

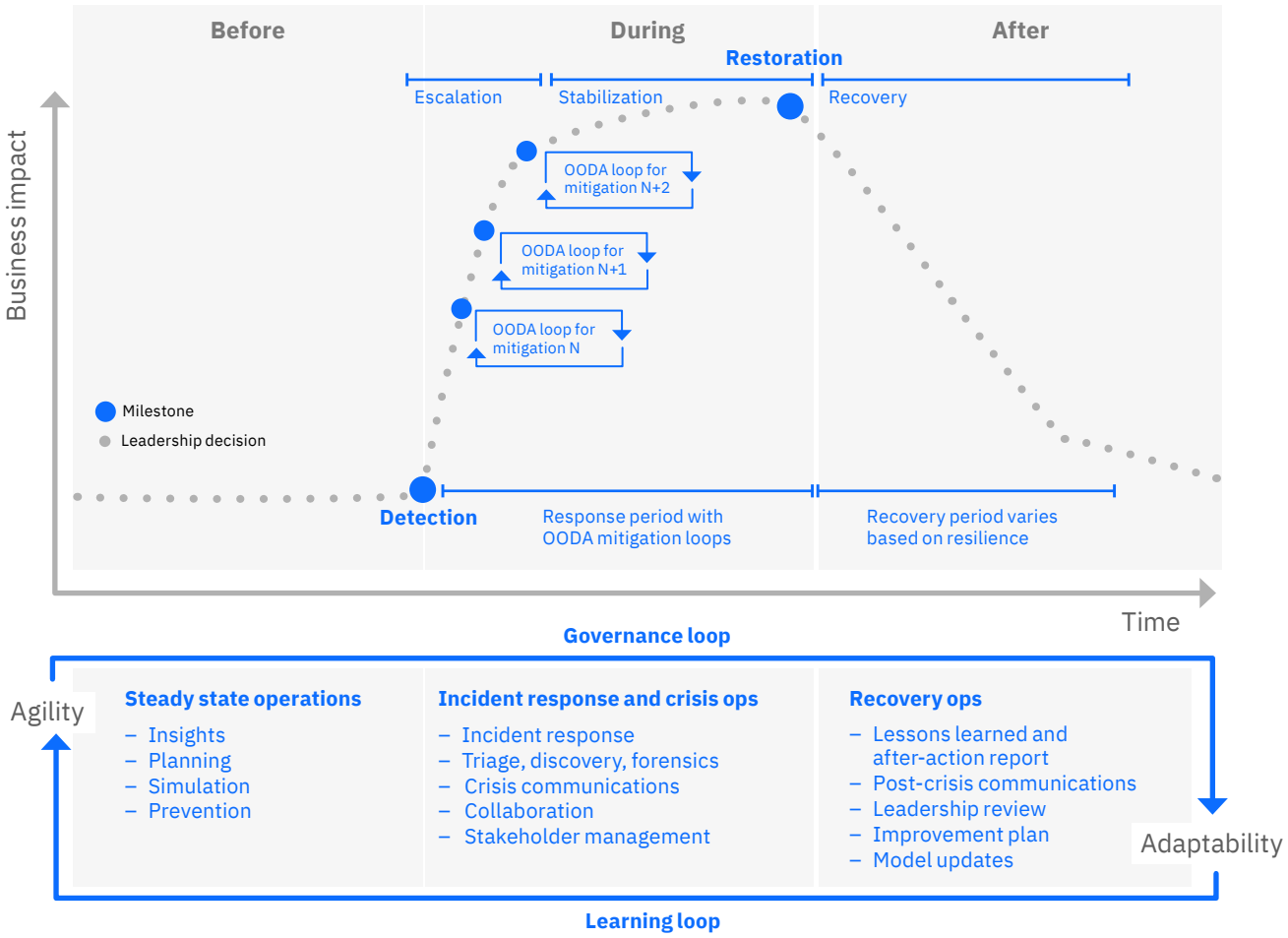
The crisis lifecycle, phase 1: Steady state/planning

As the COVID-19 crisis unfolds, organizations that have yet to experience a cyber threat still have the luxury of time – they should use it wisely. (See Figure 2.)

Most important, organizations without a CSIRP should create one. Leaders that have already been through that stage of planning should take the opportunity now to evaluate the CSIRP for any gaps based on their COVID-19 security posture. Even when a "black swan" event transforms into a longer-term reality, such as with COVID-19, there are options.[22] The key is to find ways to improve those options and buy time to make better decisions.

Figure 2

The crisis lifecycle



Source: IBM Institute for Business Value analysis.

An organization's ability to execute amid disaster can be refined using simulations. While there's no substitute for real-life, hands-on experience, simulations with drills and repetition are useful to discover any gaps in risk management and risk mitigation models. The more teams practice, the more they know what to anticipate and how they will respond during actual security events. Teams can see variables and dependencies unfold in real time, model their responses, and continue to improve.

Defining risk management

Cyber resilience is an organization's ability to prevent, respond to, and recover from a cyberattack as well as sustain the integrity of internal and external operations. The three core concerns are threats, vulnerabilities, and risk:

- *Threat:* Anything that can exploit a vulnerability, intentionally or accidentally, and commandeer, damage, or destroy an information or operational asset. These are discrete tactics or events.
- *Vulnerability:* Weaknesses or gaps in a security program that can be exploited by a threat to gain unauthorized access to an asset.
- *Risk:* The potential for loss, damage, or destruction as a result of a threat acting upon a vulnerability.[23]

The challenge, particularly in the age of COVID-19, is that risks are dynamic, emergent, and unpredictable—yet often interdependent. Risk management involves identifying threats and modeling the magnitude of operational impact in conjunction with the likelihood or probability of occurrence. That's why crisis response requires collaboration among cybersecurity, technology, and operations—a cross-functional (and increasingly cross-organizational) activity.

When risks become real, teams need to shift operations from planning and modeling to incident response, disaster recovery, and business continuity. Most importantly, it is imperative that plan/simulation processes are the same as action/response processes. The ability to make decisions quickly and collaboratively often represents the difference between success and failure.

Phase 1: Actions to take

Align operations, practice, and refine the playbook

1. Build the plan and the team. Create a CSIRP that is regularly updated to reflect the current operating environment. Validate and test crisis alert rosters to complete 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 the response plan. 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 (including unavoidable, major accident) clauses. Examine supply chain networks for fourth-party and "n-party" risk.

4. Make the plan real. Tabletop exercises and breach simulations 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 simulation 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. Crisis planning needs to accommodate a spectrum of operational disruption and social impacts, which require different approaches to crisis mitigation and response.

5. Learn from mistakes. Failure during crisis simulation is infinitely more valuable—and less costly—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.

The crisis lifecycle, phase 2: Incident response

Despite thorough plans and preparation, a crisis, by definition, strikes in unanticipated ways. When it affects organizations indiscriminately—as with the COVID-19 pandemic—systemic failure is a real possibility. In times of systemic risk, an organization's routine operational capabilities may be identified as essential to critical infrastructure, requiring significant adjustments to steady state operations.

When an actual crisis arises, teams that have used simulation drills to update response plans and refine abilities typically fare better. Because teams know what to do, leaders can observe how a situation is evolving. They can then make decisions and redirect when needed to protect the safety of employees, customers, and other stakeholders; protect data integrity; and respond to events in ways that help alleviate the particular crisis.

If crisis strikes indiscriminately and causes significant social disruption, organizations need to use operational resources in new ways to provide aid and restore confidence. With proper planning, response plans can factor in a broad range of variables and help leaders choose responses that bolster goodwill, integrity, and trust.

Crisis operations

Striking the right balance between governance and ingenuity is crucial to crisis resolution. Establishing governance guidelines for critical communications can pave the way for more creative problem solving and collaboration for more intractable crisis mitigation efforts. While problems might seem technical, almost invariably the solutions involve human sensibilities and teamwork.

When a security breach or cyberattack occurs, executives must quickly instill confidence in their customers and other stakeholders that they're doing everything possible to solve the problem. For many leaders in the C-suite, this type of fast, intuitive response doesn't come naturally. Although they might know what to do technically to manage a breach, they often aren't prepared to cope with the human side of the equation.

In mid-crisis, the playbook and simulations will enable everyone—from the security team to communications and PR professionals to the CEO—to understand their role and take appropriate action with the right mix of hard and soft skills that enable the team to get ahead of the problem.

Phase 2: Actions to take

Run the playbook, adapt, and collaborate

1. Accept that perfection doesn't exist—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. Which measures suggest progress? Would more specialized resources, more budget, or more time make a difference? How is this crisis similar to (and different from) 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.

The crisis lifecycle, Phase 3: Recovery and improvement

Some security experts suggest the COVID-19 pandemic might be instructive for future cyberattacks that could cause social disruption on similarly massive scales.[24] As Brian Finch writes in an op-ed for The Hill, "Cyber thinkers in Washington would do well then to carefully study any successful measures used to mitigate the financial impact caused by COVID-19. Doing so will help prevent unnecessary scrambling and jury-rigged solutions when the inevitable cyber pandemic arrives."[25]

COVID-19 has certainly put the world on notice. As with any great upheaval, some of the lessons learned can be used to improve future responses. One thing seems certain: the ability to communicate, coordinate, and collaborate—as much as the ability to command and control—will win the day.

With some combination of avoidance and prevention, incident response drills, and simulations, security leaders can gain both greater confidence in their ability to withstand moments of crisis and the conviction that comes from operating with integrity. According to Chris Pierson, CEO of cybersecurity firm BlackCloak, "Cybercriminals are not taking a break during this global pandemic and neither will the defenders or their suppliers, so I think the outlook is extremely positive."[26]

Phase 3: Actions to take

Invest in new capabilities to make the business more resilient and adaptable

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).[27]

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.[28]

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.[29]

5. Raise security awareness. Cyber resilient organizations prioritize security as a strategic capability across the enterprise. 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.[30]

About the authors

Wendi Whitmore

Vice President, X-Force Threat Intelligence, IBM Security
wwhitmor@us.ibm.com
linkedin.com/in/wendiwhitmore2
@wendiwhitmore

Wendi Whitmore is the Vice President of IBM X-Force Threat Intelligence and a recognized voice of expertise in the cybersecurity realm. She has over a decade and a half of diverse experience in incident response, proactive and strategic information security services, intelligence, and data breach investigations with clients from virtually every sector and geography.

Gerald Parham

Security and CIO Research Leader, IBM Institute for Business Value
gparham@us.ibm.com
linkedin.com/in/gerryparham/

Gerald Parham is the Global Research Leader for Security & CIO for the IBM Institute for Business Value. Gerald's research focuses on the cyber lifecycle and cyber value chains, in particular the relationship between strategy, risk, security operations, identity, privacy, and trust. He has more than 20 years of experience in executive leadership, innovation, and intellectual property development.

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.

Related reports

"COVID-19 Action Guide"
ibm.co/covid-19-action-guide

"A CIO's guide to extreme challenges"
ibm.co/cio-guide-challenges

"How CISOs can secure a strategic partnership"
ibm.com/thought-leadership/institute-business-value/report/ciso-strategic-partnership

Notes and sources

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

2 XF-IRIS internal data analysis. Additional COVID-19 data insights are available at https://exchange.xforce.ibmcloud.com/collection/Threat-Actors-Capitalizing-on-COVID-19-f812020e3eddbd09a0294969721643fe

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

4 "2019 Cost of Data Breach Study: Global Analysis." Ponemon Institute. Benchmark research sponsored by IBM independently conducted by Ponemon Institute LLC. 2019. https://www.ibm.com/downloads/cas/ZBZLY7KL

5 Whitney, Lance. "Cybercriminals exploiting coronavirus outbreak with virus-themed sales on the dark web." TechRepublic. March 19, 2020. https://www.techrepublic.com/article/cybercriminals-exploiting-coronavirus-outbreak-with-virus-themed-sales-on-the-dark-web/

6 "Update: Coronavirus-themed domains 50% more likely to be malicious than other domains." Check Point blog post, accessed March 27, 2020. https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/

7 "U.S Small Business Administration Spoofed In Remcos RAT Campaign." IBM X-Force Threat Intelligence. IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Small-Businesses-Seeking-Disaster-Assistance-Targeted-By-Remcos-Infostealer-e8b9f4f5e9d8c98f51e2ee09ac632ef8; "Holding Your Health For Ransom: Extortions On The Rise." IBM X-Force Threat Intelligence. IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Holding-Your-Health-For-Ransom-Extortions-On-The-Rise-1fc43fac1cf1b72a4245f0107da283e3

8 "Covid-19 Drug Advice From The WHO Spoofed to Distribute Agent Tesla Info-Stealer." IBM X-Force Threat Intelligence. IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

9 Vergelis, Maria. "Coronavirus phishing." Kaspersky Daily. February 7, 2020. https://www.kaspersky.com/blog/coronavirus-phishing/32395/

10 Whitmore, Wendi. "IBM X-Force Threat Intelligence Cybersecurity Brief: Novel Coronavirus (COVID-19)." March 17, 2020. https://securityintelligence.com/posts/ibm-x-force-threat-intelligence-cybersecurity-brief-novel-coronavirus-covid-19/

11 Stein, Shira, and Jennifer Jacobs. "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak." Bloomberg. March 16, 2020. https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

12 Miller, Maggie. "Top US health agency suffers cyberattack." The Hill. March 16, 2020. https://thehill.com/policy/cybersecurity/487756-top-us-health-agency-suffers-cyberattack-report

13 Pipikaite, Algirde, and Nicholas Davis. "Why cybersecurity matters more than ever during the coronavirus pandemic." World Economic Forum. March 17, 2020. https://www.weforum.org/agenda/2020/03/coronavirus-pandemiccybersecurity/

14 "CISA Insights." US Cybersecurity and Infrastructure Security Agency website, accessed March 29, 2020. https://www.cisa.gov/insights

15 Mervosh, Sarah, Denise Lu, and Vanessa Swales. “See Which States and Cities Have Told Residents to Stay at Home.” *The New York Times*. March 29, 2020. https://www.nytimes.com/interactive/2020/us/coronavirus-stay-at-home-order.html

16 Gettleman, Jeffrey, and Kai Schultz. “Modi Orders 3-Week Total Lockdown for All 1.3 Billion Indians.” *The New York Times*. March 24, 2020. https://www.nytimes.com/2020/03/24/world/asia/india-coronavirus-lockdown.html

17 Miller, Maggie. “Zoom vulnerabilities draw new scrutiny amid coronavirus fallout.” The Hill. April 2, 2020. https://thehill.com/policy/cybersecurity/490685-zoom-vulnerabilities-exposed-as-meetings-move-online

18 Seals, Tara. “Coronavirus Poll Results: Cyberattacks Ramp Up, WFH Prep Uneven.” Threatpost. March 19, 2020. https://threatpost.com/coronavirus-poll-cyberattacks-work-from-home/153958/

19 “Federal employees may soon be ordered to work from home.” *The Washington Post*. March 13, 2020.

20 “OODA loop.” Wikipedia, accessed April 1, 2020. https://en.wikipedia.org/wiki/OODA_loop

21 “The 2019 Cyber Resilient Organization.” Ponemon Institute and IBM. 2019. https://www.ibm.com/downloads/cas/GAVGOVNV

22 Black swan events describe entirely unexpected situations outside the realm of normal expectation that have extreme consequences. Taleb, Nassim Nicholas. “The Black Swan: The impact of the highly improbable.” 2007.

23 “Threat, vulnerability, risk—commonly mixed up terms.” Threat analysis Group website, accessed April 1, 2020. https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/

24 Kallberg, Jan, and Col. Stephen Hamilton. “What COVID-19 can teach us about cyber resilience.” Fifth Domain. March 2020. https://www.fifthdomain.com/opinion/2020/03/23/what-covid-19-can-teach-us-about-cyber-resilience/

25 Finch, Brian. “Cyber planners should be carefully watching the coronavirus.” The Hill. March 2, 2020. https://thehill.com/opinion/cybersecurity/485391-cyber-planners-should-be-carefully-watching-the-coronavirus

26 Ferguson, Scott. “Cybersecurity Sector Faces Reckoning After Coronavirus Hits.” BankInfoSecurity. March 10, 2020. https://www.bankinfosecurity.com/coronavirus-hits-wall-street-cyber-survive-slide-a-13913

27 “2019 Cost of Data Breach Study: Global Analysis.” Ponemon Institute. Benchmark research sponsored by IBM independently conducted by Ponemon Institute LLC. 2019. https://www.ibm.com/downloads/cas/ZBZLY7KL

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

29 “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

30 “The 2019 Cyber Resilient Organization.” Ponemon Institute and IBM. 2019. https://www.ibm.com/downloads/cas/GAVGOVNV

About Research Insights

Research insights are fact-based strategic insights for business executives on critical public and private sector issues. They are based on findings from analysis of our own primary research studies. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

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

44031444USEN-01