Gartner Research

Be Resilient: Prepare to Treat Cyber Risk Following (COVID-19) Outbreak by Focusing on These7 Areas

Richard Addiscott, Sr Director Analyst
David Gregory, Sr Director Analyst
Sam Olyaei, Director Analyst
Katell Thielemann, VP Analyst
Bart Willemsen, VP Analyst
Felix Gaehtgens, VP Analyst
David Mahdi, Sr Director Analyst

17 April 2020

Gartner

Be Resilient: Prepare to Treat Cyber Risk Following the Coronavirus (COVID-19) Outbreak by Focusing on These 7 Areas

Published 17 April 2020 - ID G00722616 - 22 min read

By Analysts Richard Addiscott, David Gregory, Sam Olyaei, Katell Thielemann, Bart Willemsen, Felix Gaehtgens, David Mahdi

Initiatives: Security and Risk Management Leaders **and 1 more**

During pandemics, organizations are focused on employee health and business continuity. Security and risk management leaders must take preemptive steps to ensure the resiliency and security of their organization's operations as attackers seek to exploit human nature and nonstandard operating modes.

Overview

Key Challenges

- During extended business disruptions caused by global events, such as the COVID-19 pandemic, business operations ensue in nonstandard manners. Employees who are naturally concerned about their own health and that of their families may be more susceptible to phishing and other socially engineered attacks seeking to exploit heightened anxiety about the effects of the coronavirus.
- Employee dispersion will mean documented cybersecurity incident response protocols based on a set of known operational protocols, facilities and communication channels become obsolete.
- Organizations whose cybersecurity operations and monitoring capabilities cover only a portion of their standard operating environment will be further impacted, as workers relocate to new premises or to a remote working model that expands the scope and complexity of the operating environment.
- Vendors and other partners who provide security services and capabilities will also be impacted by the same business disruption and may not be able to provide the same level of service and support as they would under normal operating conditions.

Recommendations

Security and risk management leaders responsible for ensuring information security is maintained during the coronavirus (COVID-19) pandemic should:

- Refine security monitoring capabilities to reflect an operating environment where network traffic patterns, data and system access vectors have changed due to increased remote and mobile operations. Reengineer incident management workflows to respond to cybersecurity events when usual response facilities and communication channels may not be available.
- Communicate key security awareness messages to ensure the organization's workforce remains vigilant and alert to phishing and other socially engineered cyber attacks that could compromise operational continuity, data security and privacy when working remotely.
- Engage with partners and vendors to understand the potential impacts to the availability of critical security services and their security capability and capacity. Check with vendors to see what, if any, complementary services or additional functionality they are offering to assist organizations operating during the COVID-19 pandemic, and apply them where appropriate.
- Ensure that measures taken extend beyond pure IT security and include a focus on compliance and cyber-physical systems where necessary.

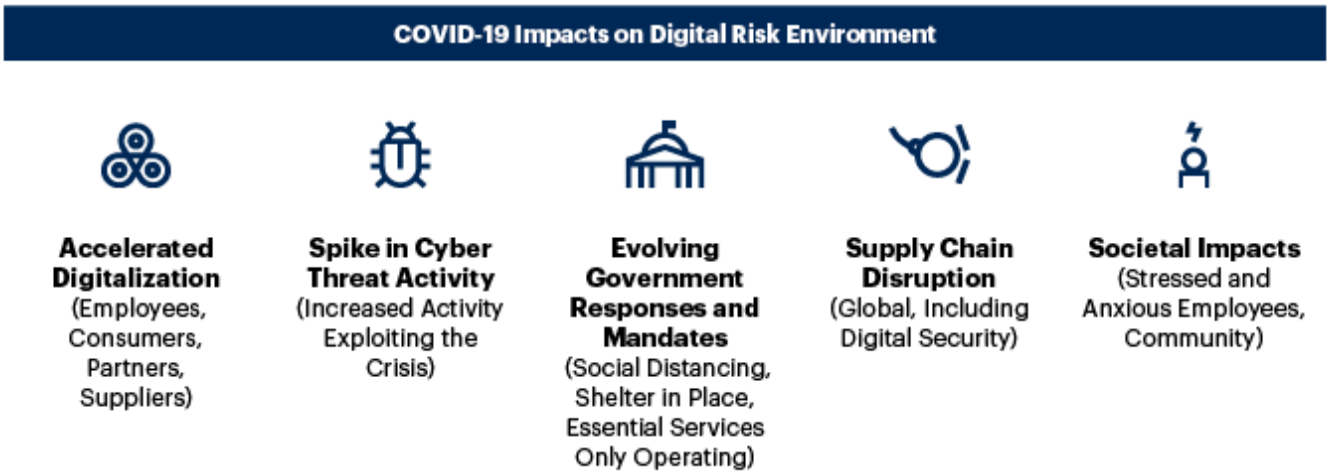
Introduction

As organizations are trying to maintain a semblance of stability while their workforce works from living rooms and dining rooms dispersed across the globe, the ramifications of the world's response to the coronavirus will have profound and unclear impacts on security and risk management (SRM). SRM leaders confront an intensely dynamic setting where risk is far greater, and where leaders nevertheless must continue to protect their organizations, employees and partners. In this time of increased uncertainty, we advise an approach that emphasizes resilience and focuses risk mitigation efforts on what SRM leaders know today and prepares for what could happen tomorrow.

As highlighted in Figure 1, Gartner sees several coronavirus-related factors (not an exhaustive list) that are shaping an organization's digital risk environment. We know that more, already anxious, employees than ever are working remotely from home, a condition that could have serious implications for remote worker security and/or privacy regulation compliance. [1] We know that phishing attempts are increasing with no sector or technology stack immune from attackers, [2] targeting COVID-19 responses and anxieties. [3] It may be likely for a ransomware attack to impersonate a corporate executive and instruct employees — now distant and isolated at home — to turn over vital passwords or financial information. Further, in our increasingly connected world, vulnerabilities, threats and risks now live along a cyber-physical spectrum, and COVID-19-induced business operating model disruptions will exacerbate the problem.

Figure 1. The COVID-19 Factors Shaping the Digital Risk Environment

The COVID-19 Factors Shaping the Digital Risk Environment



Source: Gartner
722616_C

These correlated factors are seemingly coming together in a perfect storm of external environmental conditions that are amplifying the organization's operational risks, not just cybersecurity, and they must be responded to immediately to ensure the long-term viability and health of the organization. Accordingly, these factors will need to be considered by SRM leaders as they seek to provide assurance to their senior executives that they are taking reasonable steps to address any risks to the organization's digital operations and operational resilience during the coronavirus pandemic.

There are seven key areas that SRM leaders need to focus on in the short to medium term to ensure that their organization is as prepared as possible for what could be an extended period of business disruption as the world responds to the coronavirus pandemic.

Analysis

Focus Area 1: Ensure the Organization's Incident Response Protocols Reflect the Altered Operating Conditions and Are Tested Early

In a pandemic scenario where the cybersecurity incident response team is operating remotely or from home, incident response plans and protocols will likely become obsolete or need considerable change. Failure to adapt your cybersecurity incident response protocols to reflect the altered operating conditions during the COVID-19 pandemic could severely limit your organization's ability to respond effectively to even the most common, usually well-managed incidents.

Gartner recommends that SRM leaders undertake the following steps as soon as possible to ensure their cybersecurity incident response capabilities can perform effectively to limit the impact of a security incident even if the organization's response team is operating remotely and does not have access to the facilities and systems they are used to using:

- Review the response team's roster and roles to confirm all primary, secondary and alternate roles are filled and that those in the roles are healthy and have all the minimum equipment required to perform their respective roles effectively. Ensure contact details for senior stakeholders (especially those on the crisis management team) are still valid, tested and, where required, amended to ensure all critical stakeholders are contactable in the event of an incident.
- Ensure all contact details for law enforcement, emergency services and key IT vendors are up to date.
- Ensure all documentation, such as playbooks and running sheets, are available from a centrally located repository that is available to all team members remotely (for example, Microsoft Teams and Slack).
- Conduct a walk-through of relevant incident response plans as if operating under the revised operating conditions. Note and remediate any glitches that hamper the effectiveness of the new working arrangements and retest those aspects, at the very least, as soon as possible.
- Contact your usual equipment providers (such as server hardware and laptops) to see what, if any, stock they have available, and if they can get it to you, where there is a need to swap out equipment to restore services. If in doubt, also undertake a quick inventory of existing infrastructure to see if there is any spare or underutilized IT equipment that could be used in the event of a failure.
- If one has been developed, ensure that your organization's media communications protocols are in place. This could include pre-prepared media holding statements, staff media policy and social media monitoring. Identify who the organization's senior spokesperson is and confirm they have been trained to provide media briefings with support from the organization's communications or media liaison department.

For those organizations that have little or no cybersecurity incident response capability, it may be difficult or too late to stand up a whole new capability using internal resources. In this scenario, SRM leaders should consider acquiring the services of a managed security services provider that, based on a retainer, can assist in the event of a cybersecurity incident.

Use these Gartner resources to assist your cybersecurity incident response planning and testing activities:

- "3 COVID-19 Scenarios for Fast Tabletop Exercises"
- "COVID-19 Tabletop Exercise Facilitators Guide"
- "Toolkit: Security Incident Response Scenario for Phishing Attacks"

Focus Area 2: Ensure All Remote Access Capabilities Are Tested, Secure and Endpoints Used by Workers Are Patched

An organization's security team can be caught out when there's a sudden, at-pace migration of workers from an on-premises to remote working operating model. In the rush to have people out of the office, there may not be enough time to perform the usual basic endpoint hygiene and connectivity performance checks on corporately owned devices before they are off the corporate network for an extended period. Additionally, it may be that there are not enough laptop devices to go around to all remote workers, and using their personal devices for work is a necessity, at the very least, until they can be supplied with a fresh laptop. SRM leaders should undertake the following actions when faced with this situation:

- Ensure any organizationally provided endpoints, such as laptops, have the minimum viable endpoint protection configurations for off-LAN activity (for example, signature updates are received directly from the cloud). If you do not have the latest version of your endpoint protection platform (EPP) solution, upgrade new devices to the latest version and plan for a migration of the remainder. Many suppliers are offering assistance to audit current configurations and migration assistance to upgrade.
- On-premises managed endpoint protection solutions do not always provide management visibility of remote PCs. Consider migrating to a cloud-managed version to improve remote visibility.
- Contact the organization's EPP vendor to see if it can provide, ideally free of charge, copies of anti-malware software to workers using their personal devices for business while working from home.
- Be cautious about providing access to corporate applications that store mission-critical or personal information and are hosted inside the network from personal, nontrusted devices unless it can be confirmed that they have an up-to-date anti-malware solution in place. For extra protection, require all access to critical systems from outside the network to use software-token-based multifactor authentication, especially where the worker is using their personal device.
- Minimize remote access vulnerabilities via single sign-on (SSO) for cloud-hosted and on-premises applications. Where SSO is not feasible, leverage password synchronisation across multiple SaaS applications.
- Audit and, where required, delete any orphaned privileged accounts. Where possible, suspend any privileged user accounts that are not directly related to mission-critical systems.
- Wherever possible, leverage data loss prevention capabilities, such as Microsoft InTune (for Microsoft Office 365-hosted information repositories) to prevent users from saving sensitive corporate information onto personal devices or printing to home printers.

- Leverage existing data classification rules to ensure your available data loss prevention capabilities are configured to protect your most sensitive data being accessed routinely by your remote workforce. Focus on ensuring the necessary protections are in place for your most critical datasets first. Capabilities such as cloud access security brokers and data encryption (for both on-premises and cloud-hosted datasets) will be key to effective data security and reduce data-security-related risk exposure arising from your remote workforce.

- Confirm with I&O teams that all remote access infrastructure (such as VPNs) are tested and have the latest vendor and security patches in place. Also ensure that these capabilities are load tested to ensure all those working remotely can connect and that their connections are stable. Enable split tunnel configurations to minimize backhaul traffic.

- Confirm with the organization's I&O team how it plans to ensure that key security processes, such as patch management, will be executed while the IT team is working remotely.

- Mandate a change freeze on all critical systems, except for critical security patches and/or emergency changes, while the IT team is working remotely. Do not ignore critical patches, as vulnerability exploit encounters will increase.

- Ensure that the security team is represented on any IT and/or business-led crisis management or business continuity working groups established to guide the organization's digital operations during the pandemic disruption. This will ensure that the security team has the ability to provide business-risk-appropriate advice that informs any significant decisions the organization takes in regard to the pandemic response. With security being represented on this working group, it also provides the opportunity to respond proactively whenever possible to enable the effective and secure execution of any actions arising from those decisions.

For those organizations under significant strain to remain viable during the COVID-19 pandemic, there may be the need to undertake drastic, often unexpected, actions to reduce costs. Where this involves the sudden reduction of an already stressed and anxious remote workforce, on a temporary or permanent basis, SRM leaders must be prepared for an increase in malicious insider activity from those whose livelihoods have been impacted unexpectedly and may seek to take retaliatory action.

In this regard, SRM leaders must work with the organization's human resources team to remain apprised of any forthcoming enforced separations. Where it is expected there will be a period of days, weeks or even months between notification (of separation) and departure of an employee, SRM leaders must ensure that security monitoring functions are alerted to any suspicious activity related to the user accounts of any departing employees.

SRM leaders must also work closely with the IT team to ensure that access to corporate information and applications is suspended immediately upon separation from the organization and steps are taken to retrieve any corporately owned devices as soon as possible. Alternatively,

depending on the organization's mobile device management capabilities, there may be the ability to lock down a device to stop the separated employee from accessing it and sensitive corporate information until the device is collected or remotely resetting the device back to factory settings.

For further guidance on ensuring the effectiveness and security of remote working capabilities, see:

- "Solving the Challenges of Modern Remote Access"
- "Key Considerations for Implementing a Work from Home Program and Reducing Risk"
- "Technology Insight for Phone-as-a-Token Authentication"
- "Toolkit: Remote Worker Policies"

Focus Area 3: Reinforce the Need for Remote Workers to Remain Vigilant to Socially Engineered Attacks

As workers transition to working from home, potentially for an extended period, there is a likelihood that they may become more relaxed when working in the warm familiarity of their own homes. For those working from a home where there are young children also sequestered from school, the home working environment may come with several boisterous distractions that impact the ability to focus and, therefore, productivity during their working day. This reduced focus and the potential for complacency bred by familiarity could see workers more susceptible than usual to socially engineered cyber attacks from a cybercriminal community looking to exploit heightened anxiety related to the COVID-19 pandemic. Security and risk management leaders need to take the following steps to ensure the now remote workforce is reminded in earnest of the need to be alert to attempts to compromise user devices and credentials.

- Take measures to extend remediations for data exfiltration scenarios to include current and near-future remote work arrangements for employees and third parties. As soon as reasonably possible, review existing remote working policies to include information protection requirements and amend as required.
- Request a meeting specifically with or arrange to reach out to senior executives. Apprise them about targeted phishing attacks, offering guidance and financial assistance for COVID-19 from government agencies and industry forums.
- Issue a targeted email to all staff alerting them to the escalating cyberthreat environment and to remind them of the need to remain focused and hypervigilant to phishing emails and other suspicious communication while working from home. Ideally, repeat these warnings on a fortnightly basis and remind the workforce of the presence and location of relevant policies, such as those related to remote and mobile working, should they have any questions.
- Provide clear guidance on who to contact and the information they need to collect should they experience a suspected compromise. Make sure any communications also provide locations to

any security awareness training relating to phishing, smishing, other socially engineered forms of cyber attacks as well as how to set up secure home networks and physically secure devices.

- If there is no security awareness training program in place, look to leverage any free or low-cost resources that might have been made available by vendors in the security awareness training marketplace. Work with the organization's human resources and health and well-being teams to ensure any regular, ongoing communications related to safe remote working include tips on how to work securely from home.
- If the resource capacity exists, consider setting up a dedicated security hotline or portal where the workforce, regardless of working arrangements, can contact the security team to ask questions and receive as close to real-time responses to security-related questions.

For further insight see:

- "Protecting Against Business Email Compromise Phishing"
- "10 Ways to Improve Security Awareness on a Tight Budget"
- "How to Stop COVID-19 (Coronavirus) Phishing Emails From Infecting Your Enterprise Network"

Focus Area 4: Ensure Security Monitoring Capabilities Are Tuned to Have Visibility of the Expanded Operating Environment

For those organizations whose cybersecurity operations capabilities are tuned to monitor events from their standard operating environment, the abrupt shift to a predominantly remote operating model could see events of cybersecurity interest being missed by the cybersecurity operations team. This will in large part be a result of the relocation of workers to new premises or to a remote working mode that suddenly expands the scope and complexity of the operating environment.

Security and risk management leaders should take the following steps to ensure that the organization's security monitoring tools and capabilities are configured to provide maximum visibility over the new expanded operating environment:

- Refine and configure internal security monitoring capabilities and log management rule sets to ensure the security operation team has full visibility of a new operating environment where risk exposure and threat activity; network traffic patterns; users, data and endpoint locations; data and system access patterns; and vectors have changed due to increased remote and mobile operations.
- Ensure all internal cybersecurity operations personnel have their access configured (and tested) to any on-premises and or cloud-based monitoring tools required so that they can perform their security monitoring duties remotely.

- Where possible, leverage privileged session management (PSM) capabilities to monitor (and manage, as necessary) any user activity involving escalations to access permissions. Pay particular attention to privileged account sessions to determine if there are any unaccounted-for deviations in usual privileged account sessions and privileged account user activity.
- If the organization's security monitoring services are outsourced to a managed security services provider, engage with them as soon as possible to ensure that they have their monitoring tools configured to monitor and collect logs in a manner that reflects altered and increased volume of external access source requests and the altered network traffic patterns.

For further insight see:

- "How to Develop and Maintain Security Monitoring Use Cases"
- "Toolkit: Communicating Effective Security Use Cases to Your MSSP or MDR"
- "IAM Leaders' Guide to Privileged Access Management"

Focus Area 5: Engage With Security Services Vendors to Evaluate Impacts to the Security Supply Chain

Your organization is not the only one feeling the impacts of the coronavirus pandemic. Those organizations that provide your organization services will also be having to take steps to ensure the health of their workforce and their operational resilience. Security and risk management leaders must have a clear understanding of the resilience of their security capability supply chain during the coronavirus pandemic.

To assess the resilience of their security capability supply chain, security and risk management leaders should undertake the following steps:

- Contact each of your major security vendors to understand what, if any, COVID-19 response plans they have invoked and how this may impact their ability to provide services to their clients. Especially for critical security vendors, ask them to provide you with an overview of their response to the pandemic to allow you to assess what, if any, impacts there will be to your ability to operate your security capabilities in an effective and efficient manner.
- Confirm how your key security vendors will be ensuring the security of any of your organization's data that is collected, stored, processed and used inside their environment to deliver their services as part of their business continuity program.
- Where it's assessed that a security vendor's services or support will be diminished during the pandemic and/or their security practices won't meet your expectations, determine if the organization's revised risk exposure exceeds the organization's risk appetite.

- For a security technology or application or service that is part of your organization's primary detection or response strategy for crown jewels or business-critical assets:
  - Identify potential replacement products and from where to acquire them.
  - Work with your colleagues in procurement and I&O to develop a high-level acquisition and implementation plan for that product in the event that your current provider falls over.

- If the organization's revenues are impacted significantly due to the coronavirus pandemic, consider asking your vendor for a freeze on payments or for reduced payment amounts until the conditions change and any dispensations allowed can be reimbursed as cash flow returns to normal.

For further insight see:

- "Coronavirus Requires Supply Chain Leaders to Adopt Enhanced Decision-Making Abilities"
- "Coronavirus Alters Supply Chain Dynamics Impacting People, Products and Costs"
- "Get Ahead of the Expanding Risk Frontier: Supply Chain Security"

Focus Area 6: Account for Cyber-Physical Systems Security Challenges

A pandemic stresses all aspects of global economies, and particularly organizations aligned to critical infrastructure sectors every citizen depends upon. The healthcare and life science industries are clearly experiencing extreme demand. So are the food, beverage, transport and logistics industries, and the telecommunications industry is also coming under sustained pressure due to the increased demand for stable bandwidth as more organizations rely on consumer-grade connectivity to maintain their operations.

Across these industries, Gartner has seen significant investments in automation and operational digitization efforts in the last decades as a result of OT/IT convergence or deployment of new connected devices or systems.

CPSs are also being deployed to help fight the pandemic, as occurred with robots deployed in Chinese hospitals. [4] These innovative systems will themselves need to be designed, deployed and operated securely and safely.

Unfortunately, it is clear that attackers are prepared to target organizations across all industry sectors in a bidirectional cyber-physical mode, including those that are in the front line in the fight against the coronavirus. Early examples include a cyber attack on a hospital in the Czech Republic, resulting in the need to halt all surgeries in the middle of fighting COVID-19, [5] and a German food delivery company falling victim to a DDoS attack. [6] Cyber-physical concerns around remote work

are also starting to emerge, with top legal firms warning their staff working from home to disable smart speakers and voice assistants such as Alexa. [7]

CPSs must feature in short- to medium-risk mitigation activities. The focus must be on ensuring foundational CPS/OT security hygiene practices, such as:

- Prioritizing asset discovery, inventory and network topology mapping.
- Evaluating the risk of fixing a vulnerability against the risk, likelihood and impact of an attack in order to prioritize scarce resource deployments.
- Reviewing access control and management policies/approaches.
- Reviewing current microsegmentation, virtual segmentation and firewall efforts.
- Focusing on endpoint hardening and open port restrictions.
- If the organization decides to increase remote operations, map all remote connections; evaluate remote access vulnerabilities, audit trails and password vaults; and track valid credentials to ensure they are not stolen from employees or third parties.
- Take advantage of free temporary offerings. Examples include SCADAFence Platform (continuous OT network monitoring that provides visibility), Waterfall (unidirectional security gateway remote screen view).
- Ongoing communications will be the glue that holds the ongoing crisis management of a pandemic response together. Employees feeling disconnected or concerned about their situation may not be as vigilant to the threats of phishing attacks. Deploy solutions provided by the EMNS and crisis management vendors to aid ongoing employee and management communications.

Focus Area 7: Don’t Forget Employee Information and Privacy

SRM leaders who also have oversight of their organization’s privacy function (or who have at least a role to play alongside the organization’s privacy team) must also consider the implications for privacy when managing the organization’s response.

Any information an employer wishes to collect from employees in relation to COVID-19 is firstly governed by the relevant jurisdictional or industry laws. Such collection/request of information should also be balanced against protecting the privacy of (potentially) affected employees, as health-related information is sensitive information of a special category. Employers can record that an employee has recently visited a risk area and/or is home with an illness.

SRM leaders need to keep in mind the following security and privacy best practices that they will have a key part in supporting:

- Record only information that is factual
- Record only the minimum amount of information necessary
- Store the information in a secure manner and limit access to that information to only those employees on a strict need-to-know basis
- Only disclose information to external parties where it is required by law (for example, to a local health agency in order to comply with a requirement under health legislation)
- Only use the collected information for specific, limited purposes (do not allow scope creep)

Determine and define the threshold values for changes applied during the crisis, to assess whether the added measures must continue post-pandemic or whether they can be retracted. For example, additional close tracking and monitoring of employees in the field should likely be removed post-pandemic, as it is disproportional to a normal situation. In other cases, such as remote work in specific functions, it may have proven beneficial and become part of the new normal. The key is that such decisions are subject to a (frequently revisited) privacy impact assessment (PIA).

For further insight, see:

- "COVID-19 Coronavirus and Employee Privacy"
- "Toolkit: Assess Your Personal Data Processing Activities"
- "Beyond GDPR: Select and Control Your Service Providers to Ensure Privacy Protection"

Security and risk management leaders who can direct their team's efforts toward the seven focus areas above are likely to be more effective over the short to medium term, as their organizations continue to adapt to a new way of working. However, over the longer term, the impacts from this significant business disruption will require additional, more strategically focused work from SRM leaders. This work, including cost optimization and a reevaluation of any in-flight security programs, will be key to ensuring their security function is ready to assist the organization as they return to normal business operations and evaluate how to ameliorate any bottom line impacts caused by the pandemic.

Evidence

"Statement by the EDPB Chair on the Processing of Personal Data in the Context of the COVID-19 Outbreak," European Data Protection Board.

"My Sick Employee," Autoriteit Persoonsgegevens.

[1] "Coronavirus Anxiety: Recognising the Impact a Pandemic Can Have on Your Mental Health," ABC News.

[2] "COVID-19 Pandemic Drives Spike in Phishing Attacks," Security Boulevard.

[3] "Widespread Reports of COVID-19 Malicious Scams Being Sent to Australians," Australian Cyber Security Centre.

[4] "Coronavirus: Hospital Ward Staffed Entirely by Robots Opens in China," NewScientist.

[5] "Czech Hospital Hit by Cyberattack While in the Midst of a COVID-19 Outbreak," ZNet.

[6] "DDoS Attack Targets German Food Delivery Service," Dark Reading.

[7] "Locked-Down Lawyers Warned Alexa Is Hearing Confidential Calls," Bloomberg.

Recommended for Gartner Clients

The Risks of Remote Work: Cybersecurity

The Pillars of Pandemic Planning

Protecting Against Business Email Compromise Phishing

IAM Leaders' Guide to Identity Governance and Administration

Facing New Vulnerabilities — Cyber-Physical Systems

How to Stop COVID-19 (Coronavirus) Phishing Emails From Infecting Your Enterprise Network

Securing the Fully Remote Workforce

Video: Pandemic Plan Guidance for Organizations

CISO Communication During COVID-19

Stop Letting Others Off the Hook

This complimentary research is part of Gartner's ongoing coverage of the business impact of the coronavirus (COVID-19).

Access additional free content and coverage at gartner.com/smarterwithgartner and gartner.com.

Talk to a Gartner Expert Today

Get access to this level of insight all year long — plus contextualized support for your strategic priorities — by becoming a client.

gartner.com/en/become-a-client

U.S.: 1 800 213 4848

International: +44 (0) 3331 306 809

About Gartner

Gartner, Inc. (NYSE: IT) is the world's leading research and advisory company and a member of the S&P 500. We equip business leaders with indispensable insights, advice and tools to achieve their mission-critical priorities today and build the successful organizations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 15,000 enterprises in more than 100 countries — across all major functions, in every industry and enterprise size.

To learn more about how we help decision makers fuel the future of business, visit gartner.com.

Gartner®