COMPUTING edge

- Security and Privacy
- Data
- Internet
- Artificial Intelligence

OCTOBER 2020

www.computer.org

IEEE COMPUTER SOCIETY

IEEE

DEPARTMENT: FROM THE EDITORS

This article originally appeared in
IT Professional
vol. 22, no. 3, 2020

IT Risk and Resilience—Cybersecurity Response to COVID-19

Tim Weil, *SecurityFeeds LLC*
San Murugesan, *Western Sydney University*

The rapid and worldwide spread of the coronavirus and its illness known as COVID-19 has made huge impact on almost everything has taken us all by surprise. We all are now experiencing a major unprecedented and unexpected global public health crisis. This pandemic has also triggered huge social upheavals, disrupted almost every industry, and impacted the life and work of everyone in almost every country. Businesses and educational institutions are closed, many employees are forced to work from their homes, supply chains have been disturbed, people are being required to self-isolate, and most travel, in-person meetings, and conventions have been banned. These disruptions could continue for months, and the resulting economic, business, and social impact will last for years.

Nevertheless, business operations and services must continue on, effectively and uninterrupted. IT has been employed in novel and traditional ways to meet these challenges. Migration of many operations and services online for remote work has become inevitable, and technologies, such as cloud computing, robots, drones, AI, chatbots, VPN, virtual dashboards, autonomous systems, and the Internet facilitate this digital transformation. IT has now taken a central role in every activity and has become an epicenter of operations in healthcare, business, education, governance, judiciary, community service, and more. What and how we do our daily personal and business activities are significantly transformed with the aid of recent developments in IT, as outlined in Table 1. It is very likely that even after we successfully emerge from the crisis, business will not be "as usual" and we may continue new ways of working and offering various services.

The COVID-19 epidemic impacted IT too, primarily positively, benefiting IT industry and IT professionals and serving public goods. However, there are a few negative impacts as well, such as increased and novel cybersecurity threats and risks, performance issues due to significantly increased workload, and business continuity (BC), which the IT industry has tackled satisfactorily.

In this context, we, IT professionals and business executives, have to critically examine the following key questions:

- Are the IT industry and other enterprises prepared for this makeover or change, and how well?
- How has the IT industry responded to explosion in demand for traditional and newer services? What innovations has this epidemic brought about? What else can we do?
- Did this crisis expose cracks in our current IT planning and offerings, and business/IT risk management? What are they?
- What has been the impact on its performance of significant increase in widespread use of IT?
- What are the security and other risks the new operational environment poses and how can we assess and address them?
- What lessons can we learn from responding to this crisis?

Digital Object Identifier 10.1109/MITP.2020.2988330
Date of current version 21 May 2020.

 Published by the IEEE Computer Society

TABLE 1. Global transformation caused by the coronavirus.

Industry	Response/Impact	Response	Underlying technology/ operation
Education	Widespread closure of educational institutions; access to labs is restricted; projects have been mothballed; and fieldwork interrupted	Virtual learning environment (online teaching, presentation, assessment, and consultation); convocation online	Online video conferencing software, virtual labs on cloud
Healthcare	Overcrowded hospitals, inability to meet the demands on them	Contact tracing, forecasting resource requirements, allotment of scare resources based on a patient's survivability, COVID-19 vaccine development, telehealth (online consultation with a doctor or medical professional); automated diagnosis	AI, ML, cloud computing, chatbot
Business	Closure of business, avoidance ofin-person retail shopping	Adherence to social distancing, services online, work from home	Chatbot, drone delivery, online meeting software, virtual office/desktop, remote access to work
Industry	Closure of business, avoidance of in-person retail shopping	Work from home, remote operations, automation and autonomous operation	Robots, automation, 3-D printing
Retail	Stores closed, only online service, avoidance of retail shopping	Online shopping, home delivery	The Web, online payment, contactless payment
Government	Spike in demands from citizens for assistance, disruption to normal operations	Migration to online services	Cloud, the Web, online meeting application
Entertainment	Entertainment venues (parks, cinema) closed, sports without spectators	Viewing online	Audio and video streaming, virtual reality
Personal life and social interaction	Lockdown	Indoor activities	Phone, audio and video chats, streaming, online gaming
Spirituality and religious practices	Places of worship closed	Online participation, prayers from home, worship through livestream	Audio and video streaming, virtual reality
Conferences	In-person conferences banned; virtual conferences	Online presentation and discussion	Video streaming, virtual conference software

- How will COVID-19 reshape IT, IT security, and risk assessment and management?
- How can we proactively plan to successfully handle crises that we might face in the future?

By addressing these critical questions—not only during the COVID-19 crisis, but also regularly—as a standard practice, we will be better prepared for whatever comes. In this article, we examine some of these questions. We also invite you to share your thoughts and ideas.

FIGURE 1. NIST Cybersecurity Framework.

IT SECURITY DURING THE PANDEMIC CRISIS

Pandemic events stress test IT systems, tactical security measures, and IT governance models causing strategic (long-term) disruption in the global digital fabric. The cybersecurity impact of the COVID-19 pandemic has spread to all sectors of international commerce including citizens, industry, government, and academic sectors. Cybersecurity professionals

TABLE 2. Threats and vulnerabilities caused by the coronavirus.

Threats and vulnerabilities	Online resource
ZOOM bombing	https://delta.ncsu.edu/news/2020/04/02/zoom-security-and-privacy/
Spyware and phishing	https://www.coalfire.com/The-Coalfire-Blog/March-2020/COVID-19-incites-cyber-crimes-of-opportunity
Malware and phishing	https://www.webarxsecurity.com/covid-19-cyber-attacks/
Health check—ISPs, cloud providers, UCaaS during pandemic	https://www.networkworld.com/article/3534130/covid-19-weekly-health-check-of-isps-cloud-providers-and-conferencing-services.html

are urgently responding to increased cyber threats and their responses span the spectrum of information security and privacy management capabilities.

The NIST cybersecurity framework (CSF) which consists of Identify, Protect, Detect, Respond, and Recover functions (see Figure 1) offers a lightweight model for companies to address the new threats and attack surface presented by COVID-19 cybersecurity earthquake.[1] Details of the framework and how diverse organizations used the methodology to improve their cybersecurity risk management are provided on the NIST CSF portal.[2] We use the CSF model to frame our discussion of global cybersecurity response. Our story highlights a set of tables showing the CSF method and industry response examples to illustrate that "there is a method to the madness" of our cybersecurity response to COVID-19.

IMPACT ON GLOBAL IT

Across the board, the cybersecurity industry has identified major threats, vulnerabilities, and attack vectors and responded with recommendations for risk management, continuity planning, containment, remediation, and recovery solutions. Sudden and massive migration to remote work has required business entities to equip and enable their IT systems for remote work and manage personnel in unprecedented new ways. The NIST CSF IDENTIFY function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities.[1]

INCREASED THREATS AND VULNERABILITIES

The NIST CSF Protect function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event.[3] Leveraging the COVID-19 anxiety and concerns and the absence of on-site personnel support, new attack vectors have emerged and gotten significant coverage in the media and the cybersecurity industry. Table 2 provides industry examples of the CSF PROTECT/DETECT activity. They include the following.

ZOOM Bombing—Security and privacy vulnerabilities in teleconferencing software allow trolling hackers to intercept authentication credentials and inject objectionable content (such as pornographic materials and violent images) into seemingly secure collaborative online meetings. An example of a ZOOM bombing exploit is interference with academic networks such as a thesis defense given over a university teleconference.

COVID-19 Phishing Attacks—As reported in FBI bulletins, there were fake, malicious emails that appeared to be from the Center for Disease Control (CDC). They contained malware attachments, or aimed to hijack user credentials.

Malware—An example of malware is a Corona Trojan overwriting master boot record and disabling hard disk storage. Ransomware attacks on healthcare systems have been escalating during the pandemic. Table 3 illustrates snapshots of malware and phishing attacks.

Network Availability—While performance of core communication networks and clouds remained satisfactory despite substantial increase in traffic, some collaborative applications faced spikes in service outages, as shown by the Network World example in Table 2.

The NIST CSF Detect function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events as shown in Table 3.

TABLE 3. Sample of malware and phishing attacks reported during coronavirus crisis.

Date	Description of cyberattack	Type of attacks
April 8, 2020	The exposure to compromised e-commerce websites is greater than ever. 26% increase in web skimming in March.	Malware
April 8, 2020	"Latest vaccine release for coronavirus (COVID-19)" mall spam spreads NanocoreRAT malware	Malware
April 8, 2020	NCSC advisory: COVID-19 exploited by malicious cyber actors	Social engineering
April 8, 2020	Fake COVID19 website is spreading FirebirdRAT via fake DHL emails	Malware
April 8, 2020	Rush to adopt online learning under COVID-19 exposes schools to cyberattacks	Zoom bombing
April 8, 2020	Sophisticated COVID-19-based phishing attacks leverage PDF attachments and SaaS to bypass defenses	Phishing, malware
April 8, 2020	CDC warns of COVID-19-related phone scams, phishing attacks	Phishing

Source: (Webarxsecurity Website, https://www.webarxsecurity.com.)

TABLE 4. Cybersecurity risk mitigation and response to the coronavirus.

Cybersecurity management response	Online resource
CxO Education (security architects partners)	https://security-architect.com/waking-up-to-the-new-covid-19-cybersecurity-reality/
COVID-19 Joint Acquisition Task Force	https://www.acq.osd.mil/jatf.html
US DHS Cyber and Infrastructure Agency (CISA)	http://www.cisa.govsites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf
NIST SP 800-46 Guide to enterprise telework, remote access, and BYOD security	https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

INDUSTRY RESPONSE

CEOs are often asked "what keeps you awake at night"? In response to the new COVID-19 threats, the CEO answer may well be "everything!" Strategic consulting firm, Security Architect Partners (SAP) recommends clear dialogues at the CxO management level, weaving key COVID-19 cybersecurity issues like employee morale, BC, telecommuting, or supply chain management into normal executive meetings. SAP recommendations to address top security concerns in COVID-19 times include:

- securing remote access;
- mitigating increased fraud and malware threats;
- assessing new suppliers' (and changes to existing supplier's security posture);
- protecting core information system availability and security;
- refactoring security program priorities, architectures, and budgets;
- managing work force morale; and
- aligning with business leadership.

The NIST CSF Respond function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond function supports the ability to contain the impact of a potential cybersecurity incident.[3] In the US, at the federal agency level, the use of the NIST CSF has long been incorporated into the cybersecurity management fabric of risk mitigation. As shown in Table 4, examples of agency response to the pandemic include the Department of Homeland Security (DHS) and Department of Defense information portals. Across all US government services, contingency plans have been activated and the disruption of service operations continues to

TABLE 5. Cybersecurity response to the coronavirus.

Cybersecurity risk mitigations	Online resource
Organizational resilience (Deloitte)	https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/CoronaVirus_POV_People%20Technology%20Path_Global_Final%20(002).pdf
Legacy Software (COBOL) Supporting Financial Systems	https://edition.cnn.com/2020/04/08/business/coronavirus-cobol-programmers-new-jersey-trnd/index.html
Fired Americans Send Unemployment Websites Crashing Down	https://www.bloomberg.com/news/articles/2020-03-25/fired-americans-send-state-unemployment-websites-crashing-down

be restored. In the area of remote access, NIST special publication 800-46 offer guidance on host security, information security; network security, remote access, bring your own device (BYOD) and telework.

RESILIENCE AND RECOVERY

By and large, IT services, and IT industries in almost every country are coping with the demand on them and addressing the challenges due to the COVID-19 crisis. Speed bumps ahead are expected. In conversations with Dan Blum, Executive Adviser and author of the upcoming book "Rational Cybersecurity for the Business," we discussed the challenges customers face when force-fitting VPN architectures into demanding use cases, such as privileged third party access to their hybrid-cloud infrastructures. In order to enable business applications to work exclusively through remote access, some layers of defense (provided through firewalls and network segmentation) need to be modified or removed. This is worrisome in light of multiple nation state and cybercrime actors targeting unpatched VPN systems.

BY AND LARGE, IT SERVICES, AND IT INDUSTRIES IN ALMOST EVERY COUNTRY ARE COPING WITH THE DEMAND ON THEM AND ADDRESSING THE CHALLENGES DUE TO THE COVID-19 CRISIS.

This process aligns with the NIST CSF Recover function, which identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.[1]

From what we have surveyed, there have not been major IT system/service failures despite huge unexpected demands on IT infrastructure/services. For example, the Internet did work well despite high demand on it; clouds were able to scale with demand; start-ups and major companies were able to develop and deploy novel applications to address unique needs to contain the virus spread. Even in cases, where demands on customer-facing government applications (in Australia) peaked several times, interruption was temporary; IT operational staff addressed that overnight. Software was updated to meet new requirements in a short time. For instance, in Australia, application software was updated to enable special payment to millions of people affected by the lockdown by direct payment to their bank account within a couple of days after the policy/stimulus announcement.

Organizations are migrating most of the services and operations that can be performed online/remotely. Consequently there are now many vulnerabilities affecting the remote work force (employees, third-party vendors, and home office networks). BYOD, unpatched routers, and open WiFi present wider targets for hackers and intruders.

In the context of Leavitt's System Model of People, Process, Technology and Structure, the global health crisis hits all the targets that cybersecurity programs are designed to protect. As one of many examples, the international consulting firm, Deloitte Global Technology, offers a reasonable scenario for dealing with the issues of seismic organizational change and effective BC strategy as noted in Table 5. Highlights of the Deloitte continuity strategy recommendations include the following.

- Response strategy:
  - review BC/disaster recovery plans;
  - establish a crisis management office;
  - develop a communications plan.
- Personnel management (health and safety):
  - enforce precautionary measures and revisit sick leave policies;
  - review/amend policies for remote work, including guidelines on travel;
  - plan for absenteeism.
- Continuity of operation:
  - rationalize technology projects and portfolios;
  - equip your connectivity, security, and infrastructure for new traffic and use patterns;
  - be ready for disruptions in your business and technology ecosystem.

Legacy Software Support (COBOL)

To respond to the spike in financial assistance relief to their citizens, several state government agencies in the US urgently needed COBOL programmers to update their 40-year-old software. This has shown once again the limitations of persistence of legacy software for critical infrastructure and a lack of software programmers who are able to maintain and support these applications. A CNN article (cited in Table 5) highlights the need for legacy software support as cited by governors across the country.

IT has now taken a central role in every activity and has become an epicenter of operations in healthcare, business, education, governance, judiciary, community service, and more.

On top of ventilators, face masks, and health care workers, you can now add COBOL programmers to the list of what several states urgently need as they battle the COVID-19 pandemic. In New Jersey, Gov. Phil Murphy has put out a call for volunteers who know how to code the decades-old computer programming language called COBOL, because many of the state's systems still run on older mainframes. In Kansas, Gov. Laura Kelly said the state's Departments of Labor was in the process of modernizing from COBOL but then the virus interfered. "So they're operating on really old stuff," she said. Connecticut has also admitted that it is struggling to process the large volume of unemployment claims with its "40-year-old system comprised of a COBOL mainframe and four other separate systems."

FURTHER READINGS

1. COVID-19: Your IEEE resources. [Online]. Available: https://spectrum.ieee.org/static/covid19-ieee-resources?
2. COVID-19 Through the Business Technology Lens. [Online]. Available: https://www.cutter.com/covid-19-through-business-technology-lens
3. COVID-19 and the New Leadership Agenda. [Online]. Available: https://www.bcg.com/featured-insights/coronavirus.aspx?
4. P. V. Kannan, "Customer service continuity and lessons learned during the COVID-19 pandemic," Apr. 11, 2020. [Online]. Available: https://www.linkedin.com/pulse/customer-service-continuity-lessons-learned-during-covid-19-pv-kannan/

IT HAS NOW TAKEN A CENTRAL ROLE IN EVERY ACTIVITY AND HAS BECOME AN EPICENTER OF OPERATIONS IN HEALTHCARE, BUSINESS, EDUCATION, GOVERNANCE, JUDICIARY, COMMUNITY SERVICE, AND MORE.

PLANNING FOR THE FUTURE

Infectious disease outbreaks and other forms of crisis—anticipated and unanticipated—are inevitable. However, their impact can be mitigated through better preparedness and more effective responses. History shows that changes that we adopted in a crisis are not always temporary—crises can fundamentally reshape not only our beliefs and behaviors,[4] but also business and industry in many ways. And, IT will play even more crucial role in the post-COVID era.

IT and other industries must continue to proactively plan, focus on research and development on key areas of practical relevance, and revisit and tailor their policies. They also need to revisit and amend necessary crisis management policies and IT and business risk management policies, strategies, and practices taking lessons from the current crisis.

An organization's ability to effectively respond to a disruption not only depends on how effective it was in the planning process, but also how effective it was with its preparation, trials, and the training of their staff, which is often neglected.

CONCLUSION

The COVID-19 pandemic is a wakeup call to all of us. The world, IT, and our life and work post-Corona, will not be the same. In the context of IT, the pandemic has offered opportunities; exposed weaknesses and vulnerabilities of our IT systems and IT planning and implementation; and presented us—the IT industry, professionals, and governments—a few challenges.

In this short article, we examined a few aspects of IT risks and resilience (see also the sidebar, "Further Reading"). There is lot to think about, explore, plan, strategize, and act. Share your thoughts and ideas (by sending an e-mail to the authors) and join the new IEEE Computer Society's Special Technical Community, IT in Practice, an online platform for sharing technical knowledge and professional experiences.

REFERENCES

1. "Five functions of the cybersecurity framework," NIST. Apr. 2018. [Online]. Available: https://www.nist.gov/cyberframework/online-learning/five-functions
2. "Cybersecurity framework," NIST. Apr. 2018. [Online]. Available: http://www.nist.gov/cyberframework
3. "CISA INSIGHTS: Risk Management for Novel Coronavirus (COVID-19)," CISA. Mar. 18, 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf
4. M. Reeves, et al., "Sensing and shaping the post-COVID era," Boston Consulting Group, Apr. 3, 2020. [Online]. Available: https://www.bcg.com/publications/2020/8-ways-companies-can-shape-reality-post-covid-19.aspx

TIM WEIL is currently a Cybersecurity Professional with SecurityFeeds LLC, Denver, CO, USA. He is a Senior Member of the IEEE and the Editor for *IT Professional* magazine. He is an industry-certified security professional (CISSP/CCSP, CISA, PMP, ISO 27001 Auditor) and an experienced auditor of enterprise security systems (federal, commercial). Contact him at trweil@ieee.org; http://www.securityfeeds.com.

SAN MURUGESAN is currently the Director of BRITE Professional Services, Sydney, NSW, Australia, and an adjunct professor with Western Sydney University, Penrith, NSW, Australia. He is a former Editor-in-Chief of the *IT Professional* magazine. He is a coeditor of *Encyclopedia of Cloud Computing (Wiley 2016), Harnessing Green IT: Principles and Practices* (Wiley, 2012) and other books. He is a Member of the COMPSAC Standing Committee, a Fellow of the Australian Computer Society, and the Institution of Electronics and Telecommunication Engineers and a Golden Core member of IEEE Computer Society. Contact him at san@computer.org; http://bitly.com/sanprofile.