MITSloan
Management Review

HBP# SMR878

A Comprehensive Approach to Cyber Resilience

As data becomes more critical in supporting business units and functions — and as cyberthreats grow — the responsibility for keeping that data safe must expand beyond IT.

Chon Abraham
Ronald R. Sims

A Comprehensive Approach to Cyber Resilience

Chon Abraham and Ronald R. Sims

As data becomes more critical in supporting business units and functions — and as cyberthreats grow — the responsibility for keeping that data safe must expand beyond IT.

It's hard to imagine a more challenging year than 2020 for data security. The pandemic meant that millions of employees worldwide were suddenly working from home. More severe cyberthreats — some from highly sophisticated state actors — threatened company databases. And at a regional level, natural disasters disrupted operations and supply chains.

To gauge how organizations responded to this perfect storm of cyberthreats, we interviewed 57 technology leaders during the second half of 2020, including CIOs, chief information security officers, chief data officers (CDOs), and other business leaders in public- and private-sector organizations. The key insight from that research is that cyber resilience — the ability to withstand unanticipated disruption — is no longer exclusively the responsibility of IT functions. Rather, as data becomes more pervasive across company operations and functions in improving business performance, organizations need a comprehensive approach to cyber resilience. Specifically, they need a clear plan for how to manage all aspects of data and cross-functional responsibilities for keeping that data safe.

Disruptions Continue to Grow

Most organizations were unprepared for the pandemic and the resulting shift from physical offices to working from home. Companies allowed business and function leaders to make piecemeal, ad hoc arrangements to suit the needs of their teams. As a result, IT and security teams often did not know which devices were being used by employees, the applications that were on those devices, whether they had appropriate security patches, the security of Wi-Fi connections, or the prevalence of other connected devices, such as gaming consoles and smart home devices.

The resulting free-for-all — implemented for the sake of continuing business operations — led to an exponential increase in cyber risk. Cyberattacks rose 400% in 2020 compared with previous years, primarily due to nefarious players exploiting ill-secured virtual work environments and IT infrastructures that had been adapted on the fly. [1] On average, these attacks cost businesses hundreds of thousands of dollars to address (but often far more) and are a factor

in many small and medium-sized enterprises going out of business. [2] Even with U.S. company losses due to cyberattacks nearing a reported $1 trillion by late 2020, a survey of nearly 1,000 organizations found that only 44% had cyber preparedness and incident response plans in place. Worse, just 32% said the plan was actually effective, and typically the board or the C-suite had not been engaged in developing the plan. [3]

The recent SolarWinds attack on government and Fortune 500 companies was even scarier. The attack exposed sensitive data for eight months at nearly 18,000 organizations using SolarWinds' IT management and network monitoring software. [4] Worse, the hack opened a path for other cybercriminals to follow. The extent of the damage across supply chains may not be realized for months, if not years.

There is no going back. Data is a key source of competitive advantage for companies across all industries, and the pace of digitization will only accelerate. At the same time, the threat of disruptions and deliberate attacks puts companies' data increasingly at risk. Given this complexity, companies need a comprehensive approach to cyber resilience that is grounded in data management and spans roles throughout the organization.

The Importance of Data Management

Data management is the process of accessing, storing, organizing, and maintaining the data created and collected by an organization. Companies must ensure that data is accessible, understandable, linked, trusted, and secured. [5] Moreover, data needs to be secure in transit from point A to point B across a computer network or IT environment — because network interfaces are often the key points of vulnerability to outsiders.

Addressing data management requires answers to several critical questions:

- Where does the data come from, and where does the data reside in the organization — for example, in databases, data warehouses, or data lakes?
- How frequently does data change, and how does it move throughout the organization over time?
- Who (such as IT staff members) or what (internet-of-things devices, or processes from another network) has access to data?
- How is data used? For example, is it transformed in some way or fed in raw form to critical systems in the company?
- In a crisis such as a natural disaster, how can data be easily accessed or locked down?
- If the organization faces a cyberattack, how is the data checked to determine whether it has been compromised? How does the organization trace the flow of contaminated data across the IT architecture?

In addressing all of these questions, companies need to strike the right balance between making data accessible so that business units and functions can use it to create value, and also ensuring its security. Moreover, they need to understand the landscape of potential threats and prepare for them — in terms of rapid detection, effective response, and efficient recovery. Because this is a significant undertaking in both planning and execution, the entire organization needs to be involved.

A Cross-Functional Approach to Cyber Resilience

For cyber resilience to work, IT and security teams need actionable data on everything in the network, not just the devices and applications that employees use each day. This requires up-front planning to model scenarios that will reveal how data is to be accessed, along with all possible touch points to the organization's network (such as supply chain nodes). That is a significant level of situational awareness, and it calls for a cross-functional approach across key roles.

Chief data officer. The CDO has overall responsibility for

executive-level decisions about data management, both during normal operations and in a possible breach. A key task for the CDO is creating and maintaining data classifications and categorizations for business-essential processes and associated systems.

Data stewards. The data categorizations flow up to the CDO from data stewards within each business unit and function, each of whom has firsthand knowledge of his or her department's data requirements. They know which employees require access to specific data in order to do their jobs, which systems or feeds should have access, and how operational performance would be affected if some data were unavailable or contaminated. Data stewards also validate the accuracy of the data, facilitate exchanges with other entities, and map the flow of data.

IT team. The IT team, including cybersecurity engineers and enterprise architects, are the gatekeepers of data. They define the paths by which data comes in or out of corporate systems, along with security protocols for gaining access. Notably, the IT team also trains the staff about data management, including work-from-home policies, device constraints, the rules governing company-owned hardware, and access to physical and data networks.

Human resources. The HR function has data about security clearances and work schedules, work-from-home policies, and employee requirements such as virtual private networks. This information allows the cyber resilience teams to quickly identify anomalies in workers' access to critical data and — more important — to prioritize access for certain individuals and work processes in the wake of an attack.

Legal. The legal function (including staff members working on acquisitions and partnerships) coordinates with the CDO to ensure that vendors have agreements in place stipulating realistic response times in the event of a crisis. Additionally, the legal team advises on the organization's liabilities and right to access personally owned devices sanctioned for work use in order to identify potential vulnerabilities.

Other consultants. Cyber resilience requires nontraditional support from a wide range of additional consultants. For example, epidemiologists can apply data analytics models used to track disease progression to predict how infected computer nodes could affect a network.[6] Software engineers can assess vulnerabilities in software before it gets implemented. Utility engineers, who typically work with physical infrastructure like power plants, can help organizations develop redundancy plans and alternate power supplies if they lose their primary connections. And external cyber risk consultants can play both attacker and defender in simulations to spot vulnerabilities, in addition to applying best practices from other external sources to increase an organization's defenses.

Machine learning and AI. Last, cyber resilience planning requires not only skilled threat analysts but also advanced algorithmic tools such as machine learning and AI. Increasingly, these solutions can spot irregularities and emerging threats more quickly than human operators, and at lower costs.

The growing volume of data across business functions, devices, and networks creates a clear opportunity for companies to interact with suppliers, customers, and other stakeholders in new ways that unlock value. However, that opportunity comes with a new risk of cyberthreats to the organization. By implementing clear data-management governance and adopting a cross-functional approach to cyber resilience, companies will be better equipped to protect one of their most valuable assets: their data. In addition, they will be able to understand potential threats and act in response — not in days, but in minutes. They will be able to take control, adapt, act on information that is as complete as possible, communicate well, and inspire confidence that business operations will continue and information will remain safe.

In the current environment, some organizations face almost total uncertainty regarding the near future. However, those that look forward and act proactively will be better positioned to not only survive but thrive — regardless of what comes.

About The Authors

Chon Abraham is an associate professor of information

systems at the College of William & Mary's Raymond A. Mason School of Business and a military reserve cyber officer who teaches and researches cyber resilience and governance topics. Ronald R. Sims, the Floyd Dewey Gottwald Sr. Professor of Business Administration at the Raymond A. Mason School of Business, teaches organizational behavior topics, including human resource management relative to cybersecurity and information security.

References

1. Insight on cyberattacks during the COVID-19 pandemic were derived from Federal Bureau of Investigation, "Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments," Alert No. I-040120-PSA, April 1, 2020, www.ic3.gov; and M. Miller, "FBI Sees Spike in Cyber Crime Reports During Coronavirus Pandemic," The Hill, April 16, 2020, https://thehill.com.

2. S. Steinberg, "Cyberattacks Now Cost Companies $200,000 on Average, Putting Many Out of Business," CNBC.com, Oct. 13, 2019, www.cnbc.com.

3. Z.M. Smith, E. Lostri, and J. Lewis, "The Hidden Cost of Cybercrime," PDF file (McAfee and the Center for Strategic and International Studies, December 2020), www.mcafee.com.

4. "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)," Cybersecurity & Infrastructure Security Agency, Jan. 5, 2021, www.cisa.gov; S. Wilson, "CISA Updates Guidance on SolarWinds Compromise," FedScoop, Jan. 7, 2021, www.fedscoop.com; and N. Bomey and K. Johnson, "What You Need to Know About the FireEye Hack: Cybersecurity Attack Against US Government." USA Today, Dec. 14, 2020, www.usatoday.com.

5. VAULTIS (visible, accessible, understandable, linked, trustworthy, interoperable, and secure) is the data strategy mantra and name of the U.S. Air Force Chief Data Office's data management platform. Information provided by U.S. Air Force chief data officer Eileen Vidrine, interview with authors, Jan. 12, 2021. For additional details, see L.C. Williams, "USAF Primed to Launch New Phase of Data Strategy," Federal Computer Week, Nov. 30, 2020, https://fcw.com.

6. J. Modini, T. Lynar, E. Sitnikova, et al., "Applications of Epidemiology to Cybersecurity" (paper presented at the European Conference on Cyber Warfare and Security, Chester, U.K., June 25-26, 2020); and "What Is Network Segmentation?" Cisco, accessed Feb. 24, 2021, www.cisco.com.