Organizing for Cyberresilience

A few issues back, I raised this question: Which function within a typical enterprise should be leading the development of resilience in the face of cyberattacks?[1] After some hemming and hawing about the definition of cyberresilience,[2] I suggested that functions including information security, business continuity management and business leadership might be candidates, each with potential advantages and drawbacks. I then wimped out and said that all these functions and more needed to be involved and that a program management office should take the lead.

All of which raises another question: How should businesses in both the private and public sectors organize to create resilience in the face of potentially successful cyberattacks? The key to answering this question is that cyberresilience is not anyone's job. It requires the involvement of nearly every function in the enterprise. The difficulty with this statement is that if everyone is involved, then a fairly rigorous organization of roles is necessary to keep everyone from tripping over everyone else.

STEVEN J. ROSS | CISA, CDPSE, AFBCI, MBCP

Is executive principal of Risk Masters International LLC. He has been writing one of the *Journal's* most popular columns since 1998. Ross was inducted into the ISACA® Hall of Fame in 2022. He can be reached at stross@riskmastersintl.com.

Managing Conflicting Interests

As a starting point, there is a need for a process for adjudicating conflicting interests in keeping an organization cyberresilient. For instance, the sales department might want systems to be brought back into use even if it is not proven that malware has been excised from them, while the information security function would be firmly opposed to such a move. Or human resources (HR) might emphasize retention of employees even if normal operations were impossible, but the chief financial officer (CFO) would prioritize cost reduction in a time of constrained cash flow. These are just examples of disputes I am aware of—there must be many others.

These clashing perspectives are not unique to the responses to cyberattacks. In these examples, sales did not understand operations, which could not figure out what finance was up to. And nobody understood what IT was doing. In many enterprises, the organizational response is to erect silos of data, systems, funding and personnel, regardless of senior management's expressed desire to break down the divisions between the divisions.

Collaboration in Crises

However, it has long been observed that in periods of crisis the barriers between functions disappear when they are facing common, potentially existential problems. Simply put, collaboration leads to sustainably higher performance in times of distress.[3] Teamwork, often honored more in the breach than the observance when things are going well, may become a reality when times are tough. And cyberattacks with widespread impact (i.e., destructive attacks) are extraordinarily tough for any enterprise to withstand. Sales cannot sell; operations cannot operate; accounting cannot account. The public sector is no different: The public interest cannot be served. The challenge is to create a structure for collaboration in advance of an attack so that if one should occur, the broadest overall interests will be supported.

Cyberattack Crisis Management Team

Unless decisions on responding to a cyberattack are to be referred to the chief executive officer (CEO), there must be some forum to deal with them. In

fact, there is a need for a committee to oversee both the development and execution of plans to keep an organization going should it be attacked. Many enterprises have such a committee in place to deal with crises in general,[4] which certainly would include the disruption caused by a cyberattack that downed IT systems. However, the nature of the disruption caused by a cyberattack calls for different skills and possibly for different participants in decision-making.

Because not all cyberattacks are the same, the cyberattack crisis management team (CCMT) must be flexible enough to plan for the right managers to deal with each eventuality. Disclosure of employees' personal information, for example, requires involvement by HR, privacy, legal and labor relations. Sales and operations might not have much to say. An attack on a key IT servicer—say, payroll processing—would affect everyone, though HR would necessarily take the lead with nearly all other functions responsible for managing the impact on their own personnel. A ransomware attack that incapacitated multiple functions would require all executives to determine how to weather the outage until systems and data could be restored. And, of course, whatever sort of cyberattack can be envisioned, the IT function will have a major role to play.

If an enterprise intends to make itself as cyberresilient as possible, it must confront potential attack scenarios before they occur. The CCMT might conduct formal exercises such as simulations or table-top tests. Or it might simply meet periodically to talk through the identified threats and the actions it would take if the organization were to experience a cyberattack. Of course, these preparatory measures have been—or should have been—undertaken for many years as a part of a business continuity management program and, indeed, a disruption or system outage caused by a malicious actor should be no different.

Cyberattacks and "Routine" IT Disasters

Except it is different. Many enterprises have long been prepared for outages due to weather-related events, the interruption of key utilities, fires, earthquakes and other disasters beyond management's control. The COVID-19 pandemic showed that many were able to withstand absenteeism and the inability to use business premises. But none of these negative events entailed planned, organized, targeted and malicious attacks by outside human forces on the nerve center of an enterprise. Complicating matters, an antagonist might well be a government—or a criminal gang supported (or intentionally overlooked) by a government. Most of today's managers were educated in an earlier era. Dealing with criminal attacks was not a subject when they went to business school.[5]

The nature of the disruption caused by a cyberattack calls for different skills and possibly for different participants in decision-making.

Management has had to deal with crises caused by information system outages for quite some time. But those events, as painful as they have been, were generally shorter, more easily solved and less pervasive. Plans for recovery from "routine" disasters have evolved to the point that in many organizations that I am aware of, all systems can be recovered well within the organization's tolerance for downtime. Not so with recovery from cyberattacks.[6] They take longer, call for more resources, and are more difficult to bring to a conclusive finish.

Organizing for Prior Planning

Convening the CCMT prior to an actual attack forces conflicting concerns into the open and may lead to resolution prior to the timing of need. Moreover, working through cyber-related problems in advance can identify areas of common rather than conflicting interests (some of which may be taken advantage of right away). And it helps to identify the specific responsibilities that each function must address in an attack to minimize unnecessarily overlapping efforts.

Apart from preventing cyberattacks in the first place, IT must prepare to recover systems and data from backups as rapidly as possible. Finance must plan for continued availability of cash. HR must determine how and whether to pay idled workers. Operations needs to work with vendors to ensure delivery of supplies and raw materials. Sales needs to work with customers to determine ways to keep products flowing. And some functions may just have to plan to work as best they can with whatever support they can get.

As long as all these functions organize themselves to prepare together, they are far more likely to work together should their systems be taken from them.

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Convening the CCMT prior to an actual attack forces conflicting concerns into the open and may lead to resolution prior to the timing of need.

Even more so, they are likely to manage the enterprise in a collaborative manner if they implement the organizational structures needed to survive an attack before one occurs.

Endnotes

1 Ross, S.; "Who Leads Cyberresilience?" *ISACA® Journal*, vol. 2, 2023, *https://www.isaca.org/archives*

2 *Ibid*. For reference purposes, I said that "Cyberresilience is the demonstrated ability to continue operations at an acceptable level despite any type of potential business disruption due to a cyberattack."

3 Gardner, H. K.; I. Matviak; "Seven Strategies for Promoting Collaboration in a Crisis," *Harvard Business Review*, 8 July 2020, *https://hbr.org/2020/07/7-strategies-for-promoting-collaboration-in-a-crisis*

4 This committee is often referred to as a crisis management team (CMT). There are many sources concerning the roles and responsibilities of a CMT. See, for example, Posey, B.; "Roles and Responsibilities of a Crisis Management Team," *TechTarget Disaster Recovery*, 7 April 2020, *https://www.techtarget.com/searchdisasterrecovery/tip/Roles-and-responsibilities-of-a-crisis-management-team*. This committee might also take responsibility for cyberresilience, although its membership might need to be different from one that deals with physical disasters or financial crises. For ease of discussion, let us call it the cyberattack crisis management team (CCMT) to keep the focus on this particular form of crisis.

5 But it is today. A recent survey found 23 business schools offering Master of Business Administration (MBA) or other degrees in cybersecurity in the United States alone. *Cybersecurity Guide*, "Guide to an MBA in Cybersecurity," 7 June 2023, *https://cybersecurityguide.org/programs/cybersecurity-mba/*

6 IBM, Ponemon Institute, *Cost of a Data Breach Report 2022*, USA, 2022, *www.ibm.com/downloads/cas/3R8N1DZJ*. The most recent IBM/Ponemon Institute annual study of data breach costs states that the average time to contain the impact of a cyberattack, *once the attack has been discovered*, is 74 days.