Who Leads Cyberresilience?

It seems to me that I have been reading a lot about cyberresilience these days. It is not a new issue and I have been reading (and writing[1]) about it for a long time. Currently, the proliferation of ransomware and other malware that results in extended downtime has raised concerns about many organizations' vulnerability to disruption. Simply put, it is hard to do business without information systems and the bad guys know how to hit businesses where they hurt.

Defining Cyberresilience

While there is general agreement that cyberresilience is needed, there does not seem to be universal accord as to what cyberresilience *is*. The US National Institute of Standards and Technology (NIST), usually a reliable source, says that cyberresilience is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[2] In general, others say much the same thing, but not exactly. And among the definitions in the "not exactly" category there is a world of difference.

To cite a few examples, IBM tells us that cyberresilience is "an organization's ability to prevent, withstand and recover from cybersecurity incidents."[3] So, in this company's definition, prevention is a part of resilience. Another corporate behemoth, Cisco, says that it is "an organization's ability to identify, respond, and recover swiftly from an IT security incident,"[4] with identification added to the mix.

Recovery seems to be the common element, although without clarity on what is to be recovered. Is it the compromised systems? The business supported by those systems? The data? The money lost, directly or indirectly? If in addition to recovery we add prevention and detection, what then is the difference between cyberresilience and cybersecurity more generally? I propose that it is important to answer these and other questions and to reach a common definition, because they will drive the organizational response to breaches that necessitate resilience.

I would be remiss, able to throw rocks but not catch them, if I did not offer my own definition of cyberresilience. So here goes: Cyberresilience is the demonstrated ability to continue operations at an acceptable level despite any type of potential business disruption due to a cyberattack. Note that the emphasis is on "business disruption" rather than the attacked systems.

Information Security in the Lead?

Of course, organizations should attempt to prevent cyberattacks and should detect them if they do occur. Inclusion of these activities in cyberresilience might indicate that the information security function should take the lead in developing and sustaining an organization's ability to withstand and recover from attacks. I do not see this as a natural progression: Responsibility for preventing something does not necessarily equate with leadership in recovering from it.

To be sure, the information security function has a role to play in cyberresilience. It must find out how the affected systems were undermined and ensure that the problem is fixed once the systems are brought back up. But it does not follow that information security has the appropriate expertise to make the systems—much less the business—resilient. It does not even mean that it knows how to repair the damage to the systems. If the infrastructure were compromised, then IT operations, network engineering or systems programming would be the repair persons. These functions are even

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.

ENJOYING THIS ARTICLE?

- Read *Ransomware Readiness Audit Program. www.isaca.org/ransomware-readiness-audit-program*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

further removed than information security from an organization's business operations.

Business Continuity Management in the Lead?

It might seem that I am making the case for the business continuity management (BCM) function to lead cyberresilience. This might seem to make a great deal of sense.[5] However, I find much of the relevant literature to be exhortations *to* business continuity managers to take action rather than claims *by* business continuity managers to carry the flag. I have had many such managers tell me that they are responsible for recovery from disasters, but that they have no role in IT.[6]

This is not the way it should be, in my opinion, but it is the way it is, in my experience. There are historical and organizational reasons that the split between BCM and IT has occurred.[7] Unfortunately, they tend to preclude BCM from asserting leadership over cyberresilience. (An exception might be made in those instances in which business continuity is organized as a subset of information security. This does exist in some, but not many, enterprises.)

Business Functions in the Lead?

A stronger case can be made for the functional units within an organization—that is, the business itself—to own the responsibility for the resilience of their operations should a cyberattack deny them the use of their information systems. After all, it is they who must make money, do more with less and pay the bills to keep a business going. In general, though, their expertise lies in the making, doing and paying—not in devising an alternative contingent operating model for the times that systems are down. They have neither the expertise, the resources nor the time. Many business managers I have spoken with are of the not-unfounded opinion that if IT is going to implement systems, then it ought to make plans for alternatives if those systems go down—which they do often enough on their own, without the aid of a cyberattacker.

Which brings us back to notion of IT having the leadership role in cyberresilience. As Abbot said to Costello, "first base."[8]

At this point, I could just wimp out and not offer my opinion on which function should lead the effort to develop cyberresilience. I will, but admit up front that my opinion may seem pretty wimpy. To my way of thinking, it does not matter which function takes the lead. No single function has all the tools, techniques, experience and expertise to be anointed as the leader. Or, put the other way round, resilience is an enterprisewide undertaking and all functions must work together to achieve it.

At the same time, leadership is required if only to ensure that all the pieces fit together. Modern businesses and government agencies are complex entities, so that what any one function does affects to a greater or lesser degree what others do. This is especially the case with any activity involving information systems and telecommunications, which cut across all functions. Ultimately, this makes cyberresilience a simple problem—unavailable data and processes—with a wickedly complex solution. Just saying this points to the need for a program management office and often to the use of external resources to connect all the disparate pieces of resilience.

Unanswered is the question of how the various functions should be organized prior to, during and after an attack to provide resilience. I will return to this in a future column.

Endnotes

1 For example, see Ross, S.; "It's About (Down) Time," *ISACA® Journal*, vol. 5, 2022, *https://www.isaca.org/archives*

2 National Institute of Standards and Technology (NIST) Computer Security Resource Center Glossary, "Cyber resiliency," USA, *https://csrc.nist.gov/glossary/term/cyber_resiliency*. Actually, this is NIST's definition of "cyber resiliency." No vocabulary lessons here, but the correct word is resilience.

3 IBM, "What Is Cyber Resilience?" USA, *https://www.ibm.com/topics/cyber-resilience*

4 Cisco, "What Is Cyber Resilience?" USA, *https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html*.

5 There is a good deal of literature that takes this point of view. An apt source, due to its sponsorship by a global business continuity organization, is Richmond, W. P.; "Achieving Cyber-Resilience: A Formula for Success," Disaster Recovery Institute International, *https://drii.org/viewpdffile/eyJpdiI6InRuQlJxeml*

6 Private communications to the author

7 Ross, S. J.; "Is Information Security a Threat to Resilience?" *ISACA Journal*, vol. 1, 2005

8 Wiles, T.; "Baseball's Greatest Skit," National Baseball Hall of Fame, USA, *https://baseballhall.org/discover/short-stops/greatest-baseball-skit*. If you do not know what this refers to, see the video: *https://www.youtube.com/watch?v=5FsJe4DScDs*. In fact, even if you do know what it means, you ought to watch the video.