Cyber (Business) Recovery

The last of the five core functions of the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is Recover.[1] It comes last because this function only comes into play if the previous four—Identify, Protect, Detect and Respond—somehow fail to prevent a cyberattack from occurring. There is not a lot of detail about recovery in the CSF beyond saying that there ought to be a recovery plan, that it ought to be updated based on lessons learned, and that recovery requires good communications with internal and external parties.[2] All good advice, somewhat lacking in specifics.

Cybersecurity Event Recovery

A few years after publishing the CSF, NIST did provide some guidance on cybersecurity event recovery.[3] In my opinion, this document was an attempt to explain business continuity planning (BCP) to technologists, not recovery planning itself. One sentence says this succinctly:

> *This document is not an operational playbook; it provides guidance to help organizations plan and prepare recovery from a cyber event and integrate the processes and procedures into their enterprise risk management plans.*[4]

That sentence raises many questions in my mind. Is an operational playbook needed for recovering from a cybersecurity event? What is a playbook in this context? For that matter, what is a cybersecurity event? A playbook is comprised of processes and procedures is it not? What exactly is being recovered—the technology? The data? The software? The business? How does a recovery plan get integrated into enterprise risk management? All good questions, somewhat lacking in utility.

Types of Attacks

I believe that some useful answers begin with the nature of a cyberattack and end with the nature of the underlying business. Cybersecurity events, to use NIST's phrase, are many things. They include the theft of personal information and of trade secrets. They include the theft of digital assets such as photographs, recordings and videos. Most serious are attacks that undermine the integrity of information or destroy it altogether.

The processes and procedures for recovery from each of these attacks are different. There is no recovery from the theft of information; it is already gone. All that can be done is to stop the outflow. On the other hand, if data were to be destroyed or otherwise made unavailable (i.e., ransomware[5]), there is a need to recover the data and continue the business in the meantime.

Cyber Business Continuity Planning

Many organizations have business continuity plans written to address natural and human-caused disasters. In those cases, the information is intact, but the workplace is not. A destructive cyberattack presents the exact opposite circumstances—the information is gone, but the office or remote workplace is just fine. So, in many cases, an organization's business continuity plan must be rethought and rewritten.

Development of a business continuity plan for a cyberattack is no simple matter. It needs to take into

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

Is executive principal of Risk Masters International LLC. Ross has been writing one of the Journal's most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

account the range of systems likely to be found in a modern enterprise: on-premises, in the cloud, hosted by third parties (e.g., Software as a Service [SaaS]), on the desktop and maybe even on a factory floor. Not only must a recovery plan address an attack on *any* of these, it must also consider the unavailability of *all* of them simultaneously.

Recovery of the systems and their associated data are only part of the plan, which must also include plans to keep an enterprise functioning while the technicians overcome an attack. It is easy to ask how long it would take to recover the systems and data, but a great deal harder to answer, beyond "It depends."

To complicate matters further, it is possible that some of the same people who will be carrying out the recovery must concurrently find and eradicate any malware that caused the outage in the first place. Little wonder that recent research has stated that the time for the processes of containment and repair averages 75 days—*after* the breach has been identified—for stricken enterprises around the world.[6]

Preparing for Recovery

Clearly, preparing for the recovery from a cyberattack entails the joint efforts of those responsible for cybersecurity, IT disaster recovery and business continuity management. The actual recovery involves those three plus business line and executive management. Unfortunately, as I see it, all these groups have limited experience working jointly. They barely share the same vocabulary, which makes combined activity more difficult. The very word "recover" has different meaning to a technician, a business continuity manager and a finance manager.

It is impossible for many people to comprehend the absence of application systems without understanding the systems themselves, including the infrastructure that supports them. Though it may be tough to explain networks, operating systems, middleware and interfaces to businesspeople, the effort must be made; the effort to explain complex matters intelligibly and the effort to understand the technology that underlies the way businesses are run. Likewise, technical personnel need to have insight into the way that the systems support the business.

This mutual comprehension is important because contemporary enterprises have built their systems of internal control on that technology. Perhaps that term is used most frequently in accounting and auditing circles, but the system of internal control has to be understood more broadly as the way businesses actually work in accordance with management's intentions. It means having a factory make the right goods in the right colors in the right amounts for the right customers just as much as it means ensuring that the balance sheet foots. It is fatuous to think that technology can be suddenly removed from a business without necessitating a new system of internal control, and downright ridiculous to think that it can be accomplished on the fly.

"The system of internal control has to be understood more broadly as the way businesses actually work in accordance with management's intentions."

Practical Imagination

Hence, the need to plan for cyber business continuity. Implicitly, the path to planning for recovery from a cyberattack is enterprisewide involvement. Salespeople need to work with customers to determine how they will be served by a business with lowered capacity. Finance managers need to figure out how suppliers will be paid, just as human resources needs to make sure employees get paid. Oh, yes, and IT needs to practice "bare metal restores" of key applications.

Moreover, to quote former US President Dwight Eisenhower, plans are worthless, but planning is everything.[7] His point, I believe, was that actual events never conform to the assumptions necessarily made in drawing up plans. The very essence of planning is projecting a state that does not exist derived from the current state and building in the flexibility to take account of conditions as they occur. This requires what I call "practical imagination."

There are an infinite number of potential attacks and an infinite number of consequences of such attacks. The practical aspect of planning is to reduce all possible events to a small enough set that can be realistically foreseen, with the recognition that, in all likelihood, the bad guys will do something kinda

sorta like what is envisioned, but not exactly. Then the imagination comes into play. What would be the first steps if a potential attack occurred? And then? And then? What ought to be done in advance to be as prepared as possible? File backups to be sure. Printed reports? Stockpiled PCs? And...?

Imaginations can run free…within the boundaries of the possible and the affordable. One person's vision of the future may not align with others'. That is why involving the entire enterprise in planning and preparing makes sense. The more the, well, not exactly merrier, but very necessary.

LOOKING FOR MORE?

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

Endnotes

1 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 16 April 2018, *https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf*

2 *Ibid.*, p. 43–44

3 Bartok, M., *et al.*; *Guide for Cybersecurity Event Recovery*, National Institute of Standards and Technology Special Publication (SP) 800-184, USA, December 2016, *https://csrc.nist.gov/publications/detail/sp/800-184/final*

4 *Ibid.*, p. vi

5 Ransomware is actually an attack on the integrity of the data, not destruction. But that is just sophistry. It must be treated as though data were destroyed.

6 IBM, *Cost of a Data Breach Report 2021*, USA, 2021, p. 22, *https://www.ibm.com/security/data-breach*

7 Dwight D. Eisenhower Presidential Library, Museum and Boyhood Home, The Eisenhowers/Quotes, USA, *https://www.eisenhowerlibrary.gov/eisenhowers/quotes*