It's About (Down) Time

Avid readers of this column (you two know who you are) know that I often quote the results of two annual international surveys concerning data breaches: the IBM Security *Cost of a Data Breach Report*[1] and Verizon's *Data Breach Investigations Report*.[2] Note that they both refer, though it is not explicitly stated, to breaches of data stored in electronic form for use on computer systems.

Through in-depth investigation, I determined the meaning of the word "breaches." (Er…I looked it up in the dictionary.) Breaches are infractions or violations of a law, obligations, ties or standards. They are gaps; broken, ruptured or torn conditions or areas. Breaches, in this context, imply failures of security, enabling the discovery of information that should be kept secret.[3,4] In other words, they concern the *taking* of data. What the term "breaches" does not address is the cost of the inability to operate a business because of data being *unavailable*.

The Cost of Downtime

I am not aware of any research into the cost of downtime comparable to the two referenced studies. Those reports deal primarily with intentional acts by cyberattackers and other miscreants. Although errors and accidents are also tracked,[5,6] the preponderance are malicious acts. Notably, ransomware is shown in the IBM Security study to have an average cost of US$4.62 million per incident,[7] including escalation, notification, lost business and response costs, but not including the cost of the ransom.[8] It is my belief (albeit without evidence) that for private sector organizations, the cost of not being able to conduct business operations is the overwhelming proportion of the losses, while this is not possible to calculate for government agencies. And I think the figure is too low.

In the absence of verifiable financial information on the cost of malicious downtime, let me share my calculated estimate for one incident. The ransomware attack experienced by the US company Colonial Pipeline has been well publicized. The company has annual revenues of US$1.32 billion.[9] Since gas is consumed every day of the year, the company's average daily revenues are US$3.62 million. The attack began on 6 May 2021 and lasted until 12 May 2021, so the pipeline was fully or partially shut down for at least seven days. For estimating purposes, let us assume that Colonial Pipeline was still able to move 50 percent of its gas. That would mean that it suffered more than US$9 million in revenue losses. This is one attack on one company, which is why, to my mind, the economic consequences of forced downtime overwhelm those of other sorts of cyberattacks.

Data Center, Cloud, SaaS and Distributed Downtime

But ransomware is only one source of extended downtime. Natural and human-caused outages have plagued information technology since the Eniac[10] first fired up its vacuum tubes. So, every IT executive has instituted a thorough, well-tested, up-to-date IT disaster recovery plan.

Well, actually, no. Of course, there are surely some who have. But contemporary application and infrastructure portfolios are a congeries of on-premises, cloud-based, Software as a Service (SaaS) and distributed systems. Can any organization truly say that it is confident that it can rapidly recover *all* its systems?

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.

As enterprises run fewer and fewer applications and store less and less data in internal data centers, the economic justification for the recovery plans put in place a decade ago or less becomes increasingly tenuous. It may simply not make sense to maintain an alternate data center when the primary one is being phased out. This is especially the case for those who built recoverability around commercial recovery services. (At the time of writing, one of the largest of these services has filed for bankruptcy in Canada, the United Kingdom and the United States.[11] The use of commercial hot sites may not even be an option in the near future.)

Much of what used to run on-premises is now running in the cloud or, more specifically, in data centers operated by commercial cloud service providers (CSPs). The architecture of the cloud enables rapid failover from a primary to a secondary data center should the former be incapacitated. And most, if not all, CSPs have built highly resilient sites. So, enterprises that use the cloud as their data centers must plan and pay for data centers in geographically distant regions along with sufficient bandwidth and wide-area route diversity. Not all do. Disaster recovery in the cloud is achievable but is not a given.

SaaS vendors realize that the resilience of their services is a strategic necessity, but they are not immune to downtime. Recent cyberattacks on SaaS providers have had widespread ripple effects among their customers.[12, 13] Potential buyers should ascertain whether and how their servicers ensure uptime. They should also prepare themselves to build workarounds if the SaaS applications they use should go down.

It should come as no surprise that distributed servers and personal computers can also be attacked and fail. Viruses such as Shamoon,[14] Shamoon II,[15] Petya, WannaCry and NotPetya[16] offer all the proof necessary.

The "So What?" Factor

Anyone who has read this far must be saying, "Okay, downtime is a bad thing. But so what?" There are three reasons why I consider downtime important enough to focus on it. The first is that I think it is important that we stop measuring the cost of cyberattacks only in the number of records breached and start focusing on hours of unavailable systems and data. I am certainly no fan of privacy breaches and theft of secrets. But I see hours of lost production—when profits are not being made and citizens are not being served, to say nothing of shores not being defended—as the most significant metric of the impact of cyberattacks.

It is important that we stop measuring the cost of cyberattacks only in the number of records breached and start focusing on hours of unavailable systems and data.

Second, we cannot lose sight of the fact that system downtime has many causes and targets. Mother Nature will have her way with information technology and so will human beings. Some of the latter may have malicious intent, but extended outages may just as well be caused by the lazy, the incompetent and the error-prone. Effective monitoring and quality control will help organizations withstand these sorts of folks as well as the attackers.

Finally, and, I believe, most urgently, we in IT live in a very dangerous world. There are horrible wars going on and cyberwarfare has become a predictable part of the fight. Ransomware has done a great deal of damage and costs a significant amount of money. But at least the attackers are offering (if not always delivering) to turn over the decryption key for a cryptocurrency payment. We may soon encounter attackers who encrypt data and *throw away* the key. Effective backups, well-drilled recovery specialists and business continuity procedures[17] attuned to cyberattacks may constitute survival tactics.

Endnotes

1 IBM Security, *Cost of a Data Breach Report 2021*, 2021, *https://www.ibm.com/downloads/cas/OJDVQGRY*
2 Verizon, *2022 Data Breach Investigations Report*, 2022, *https://www.verizon.com/business/resources/reports/dbir/*
3 Merriam-Webster Dictionary, "breach," *https://www.merriam-webster.com/dictionary/breach*
4 Macmillan Dictionary, "breach of security," *https://www.macmillandictionary.com/us/dictionary/american/breach-of-security*
5 *Op cit* Verizon

LOOKING FOR MORE?

- Read *IT Business Continuity/Disaster Recovery Audit Program. www.isaca.org/business-continuity-disaster-audit-program*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

6 *Op cit* IBM Security

7 *Ibid.,* as compared with US $4.24 million for global average total cost of data breaches of all sorts

8 *Ibid.*

9 Dun & Bradstreet, "Colonial Pipeline Company," *https://www.dnb.com/business-directory/company-profiles.colonial_pipeline_company.11bf157f4e91ff2d98b81cdf484d9f24.*html

10 Computer History Museum, "Eniac," *https://www.computerhistory.org/revolution/birth-of-the-computer/4/78.*

11 Sungard Availability Services, "Sungard Availability Services Takes Action to Strengthen Operating Cost Structure for Future Success," 11 April 2022, *https://www.sungardas.com/en-us/news/2022/april/sungard-availability-services-takes-action-to-strengthen-operating-cost-structure-for-future-success/*

12 I am referring to outages at *Salesforce.com* and Kronos. Daoudi, M.; "Is Your Business Prepared For the Next Major SaaS Outage?" *Forbes*, 25 June 2021, *https://www.forbes.com/sites/forbestechcouncil/2021/06/25/is-your-business-prepared-for-the-next-major-saas-outage/?sh=7acf50e657ea*

13 UKG Workforce Central, "Communications Sent to Impacted Kronos Private Cloud (KPC) Customers Beginning December, 13 at 12:45AM ET," Kronos Community, 13 December 2021, *https://community.kronos.com/s/feed/0D54M00004wJKHiSAO?language=en_US*

14 Council on Foreign Relations, "Compromise of Saudi Aramco and RasGas," August 2012, *https://www.cfr.org/cyber-operations/compromise-saudi-aramco-and-rasgas*

15 Jewkes, S.; J. Finkle; "Shamoon Computer Virus Variant Is Lead Suspect in Hack on Oil Firm Saipem," Reuters, 12 December 2018, *https://www.reuters.com/article/cyber-shamoon/shamoon-computer-virus-variant-is-lead-suspect-in-hack-on-oil-firm-saipem-idUSL1N1YH0QC*

16 Hern, A.; "WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017," *The Guardian*, 30 December 2017, *https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware*

17 Ross, S.; "Cyber (Business) Recovery," *ISACA® Journal*, vol. 3, 2022, *https://www.isaca.org/archives*