Building Resilient Systems:
Protecting Against the Fallout of Cyberwar

PRE-RELEASE**:** May 2020

"The first half of Greenberg's meticulously researched book [*Sandworm*] leaves us wondering: How long before it happens here? The second provides the chilling answer."
— Clifford Stoll, NYT bestselling author of The Cuckoo's Egg

"If your job, or even part of your job, is the secure safekeeping of data, the last two years have proven that task to be more difficult and treacherous than ever before."
— The Authors

Since January 2020 when the COVID19 pandemic began, the world has experienced the destructive power of an invisible viral infection spreading without conscience, and the cascading system failures that threaten our society. Viral spread is a reality. Cascading system failures are a reality.

The prospect of cyberwar exposes a threat of similar proportions, but the worldwide consequences could be felt in a matter of days rather than months. Warning-shot malware viruses have escaped already. Like warnings that were registered for the biological pandemic, experts are asking not if, but when a cyberwar will disrupt the planet.

If you are concerned for your organization that important digital documents, data, databases, operational information, graphics and media, or other digital information might be held ransom by cyber criminals, or that your entire on-premise or cloud storage system may be irretrievably corrupted, or that people or organizations you work with might be similarly attacked, then cyberterrorism is real and present for you. If it keeps you awake at night, the "terror" of cyberterrorism has already effectively entered your life, even if you have not been targeted directly.

The discussion which follows is an important one, especially if your company or organization is responsible for safeguarding information. If loss of that information will disrupt your operations, if it will halt critical operations, create financial liability, create negative consequences for customers and stakeholder processes, or render you liable for statutory or regulatory violations, then knowledge of the cyberterror threat, and what you can do about it, should be of primary concern.

Authors: Fred Bonner (EchoLeaf Systems), Peter Guglielmino (IBM), R. David Henze-Gongola (Henze Communications, LLC)

Prologue: Disaster at Our Doorstep

It was June 2017 that the *NotPetya* computer virus struck and became the most damaging and under-reported cyberattack ever. In Kyiv, Ukraine, it permanently locked almost all the computers in one of the largest banks—seemingly in an instant. It looked like a ransomware attack. The virus seemed to have access to every machine on the network. Soon after, it had targeted many other companies and government entities in Ukraine. One group tried to pay the 300 Bitcoin ransom the hackers requested—to no effect. Ransomware was only a ruse for the destructive exploit.

Another bank was taken down completely in 45 seconds. The virus stole passwords and used them to attack new machines on new networks. It propagated to an international shipping company, and to a multinational pharmaceutical group. The cyberattack in Ukraine caused trucks to line up outside of Port Elizabeth in New Jersey, USA — worldwide shipping was on the verge of coming to a complete standstill. The world was witnessing one of the first, massive, cascading failures—failed systems causing others to fail in chaotic, unpredictable succession. Oddly, *NotPetya* also contained a type of hidden antivirus, a way to turn off its destructive power, its discovery reverse engineered by a security analyst. The good news was that the cyber pathogen was halted after only creating tens of billions of dollars in damage, rather than trillions. The bad news was that, according to many analysts, *NotPetya* was only a test—a warning shot. News reports of *NotPetya* were limited. Authorities cited "security concerns" about disclosing the details of the attack. For a brief time, the public witnessed the active terror of an ongoing cyberwar.

Why does this story matter? Because *NotPety*a was a kind of cyber-explosion. And the cyber-shrapnel of that explosion spread worldwide at lightning speed, ignoring geographic borders, without consideration or conscience about the targets of its destruction. There was no logic to its path once it was unleashed. And those who now safeguard the world's data, from large corporations and governments, to small businesses, municipalities, and schools, can no longer hide from being possible victims of "the next attack."

How do you start to prepare? By being aware of the problem. Can individuals or organizations protect themselves today from the fallout of cyber war? Yes. In a nation-state cyber conflict that may ignore all logical and geographic boundaries, you *can* be resilient in the face of attack.

Executive Summary

Cyberterrorism is a real threat. It is a present danger to industry and to our society. However, what others viewed almost exclusively as criminal activity is now increasingly the aggressive work of nation-states or sophisticated criminal syndicates and highly capable lone actors working in concert with them. When an attack occurs, the difference between criminal extortion and nation-state disruption may be indiscernible. The difference between criminals and nation-states is that criminals are almost exclusively interested in using malware to steal data or to extort funds. The goal of nation-state hacking, while it may include extortion and theft schemes, may now also include the destruction of infrastructure and disruption of society itself.

If your job is the safeguarding of data, it is critically important to understand that the nature of nation-state attacks may not be strategically targeted. Rather, the entire point of the attack may be unbound, subtle, temporally distributed, and random destruction of data and infrastructure.

Any connected data, in any public or private facility, including (especially!) connected cloud infrastructure, may be vulnerable.

Senior writer at *Wired* Magazine Andy Greenberg has recently published the book *Sandworm*. It is an important and chilling argument that nation-states, not merely criminals, are dominating the spread of malware. “Sandworm” is the codename for the largest and most powerful group of nation-state hackers. It is but one group among many.

The new danger is that, with *today’s* technology, a comprehensive malware attack could cripple national infrastructure and society with little or no warning. Greenberg emphasizes that despite our best efforts at prevention, new attacks are nevertheless both possible and likely. Therefore, while prevention efforts are critical, so too is a strategy to recover quickly after an attack. Successful post-attack resilience will be predicated on taking the obvious step of decentralizing recovery nodes of large monolithic data centers that represent the most prevalent build patterns used by corporations and governments today.

The ability to create after-attack resilience is possible for every organization. This can be accomplished with known technology at very reasonable costs. Refusing to adopt small but critical changes can jeopardize nations, businesses, institutions, and individuals.

To be effective, recovery nodes must be independent and physically separated from any existing networks or centralized systems. Efforts to prepare for an inevitable attack are hampered by a lack of public awareness and consistent efforts by those who have been attacked to minimize their security or resilience failures. By creating many small, network independent recovery nodes, consumers, businesses, towns, schools, and government entities can build resilience in the event of a virulent cyberattack.

The Biggest Cyberthreat is Now Cyberterrorism

Sandworm is the umbrella term for the collection of hacker groups and individuals being controlled, or at least coordinated, by the Russian government. But while Sandworm is a threat, and almost all security analysts believe that the *NotPetya* attack was perpetrated by Sandworm, other state actors in North Korea, China, Iran, and other places are also a concern. The most pressing implication is that more and more hacker power is now coming from antagonistic nation-states.

State actors are impersonating or supporting criminal actors who are perpetuating cyber terrorism against businesses, municipalities, and individuals. Often embedded in this criminal activity are mechanisms of network control that would allow these state actors to destroy infrastructure more permanently and pervasively at their discretion.

Cyberthreats transcend both geographic and geopolitical borders, able to cause massive damage that goes beyond mere monetary loss. Malign actors can bring financial institutions, transportation networks, power distribution centers, medical facilities, not to mention networked security systems, to an instantaneous halt, with effects cascading to every business, government, and individual. A pervasive cyberattack can create instant societal chaos that can spread worldwide with great speed. The *NotPetya* virus was released through an accounting software update in Ukraine. Shortly thereafter, it had stopped shipping traffic in New Jersey.

In *Sandworm*, Greenberg describes in stark detail the genesis and growth of state-sponsored malware and cyberterrorism. In the past several years, numerous successful and destructive cyberattacks and several near misses have been mitigated by vigilance, and sometimes blind luck. These attacks and exploits, including *Stuxnet*, *Eternal Blue*, *Mimikatz*, *WannaCry*, and *NotPetya*, have mostly failed to make front page news. Unfortunately, headlines only come when the lights go out and "disruptions" spin into catastrophe. In fact, the shame and possibility of devastating lawsuits have created climates of fear of disclosure (even to law enforcement) of disruptions that appeared innocuous or emulated some common system troubles "best kept inhouse." In February 2020, the county of Palm Beach, Florida finally admitted to a ransomware attack that had occurred on their election infrastructure in 2016. County officials, from 2016 to early 2020, never mentioned it. The stated reason for the obfuscation? Security.

Complicating matters further, according to Greenberg, multiple instances of intentional subterfuge called "false flag" operations have been made to look as if they originate from one source, perhaps criminal hackers, while the responsible hacker group was in fact state-sponsored. This is the tradecraft, where the plausible deniability test of all such actions is the decisive Go-No-Go decision point for sponsors. A virile cyberattack that nearly brought down all core systems just prior to opening day of the last Winter Olympics in South Korea was filled with deceptive false flags. It was designed to look as if it originated in North Korea. Deeper research on the exploit and other incontrovertible facts showed that it was the work of Sandworm.

Before the publication of *Sandworm*, others presaged that cyberattacks have been the work of nation-states. In May of 2018, cybersecurity journalist Kate O'Flaherty warned in Forbes about the critical threat of state cyberterror: "The nature of warfare has shifted from physical to online, seeing a deluge of state-sponsored cyber assaults on the West," she wrote.
The issue gained global attention in April 2019 when the United Kingdom and the United States jointly issued a statement blaming Russia for recent cyberattacks. In July 2019 *Heritage.org* stated "Our adversaries are using cyberwarfare. We must be prepared." Greenberg's book amplifies these themes, but reports more broadly, through extensive interviews, about the implications of growing nation-state cyber threats.

World powers are presently engaged in a cyber war of epic proportions largely invisible to the public eye. Those who wish to develop technology for positive and pervasive use in society confront countless malicious actors looking for weaknesses in millions of lines of computer code. Developments in artificial intelligence and machine learning are imputing value to data that, once collected, had only marginal value. Big data is uncovering lethal "little data" that can devastate targeted adversaries. Today, clever defense mechanisms—whether a patch, or a new software release, or a cascade of new encryption methodologies and passwords—are simply a new puzzle for attackers to solve and exploit if they can; further, for the exploit to be useful to them, they don't have to fully succeed or succeed with every target. While both the enemy and the targets are ever changing, Greenberg and the many technologists he interviewed for his book all make the emphatic point that the prospect of cyber war is not a future threat requiring new capabilities. Existing capabilities and hacking technologies, used in new ways or through soft-bellied vectors discovered through "innocent" probes, are a present danger for disruption.

The coming war is now, and we are all caught in the crossfire.

Direct experience with virulent cascading failures indicates what might likely be lost after a massive cyberattack. Understanding that even small businesses, schools, and municipalities may be victims of the fallout, the day after the next cyber war may look like this:

- Every bit of connected data could be destroyed, sufficiently corrupted as to be useless, or no longer trustworthy
- Computers, small and large, may crash and fail to restart
- Many computers will need an entire operating system rebuild
- Backups that live on disk, flash, or SSDs in connected systems, themselves just data connected to computers, are vulnerable and may be deleted, encrypted, or destroyed
- Small but essential things like network routing tables could be gone
- Cloud infrastructure could be degraded or destroyed
- More subtle and less visible systems may be corrupted, but with lingering and devastating effect. This could include alteration of data or programs crucial to life support or other mechanisms that may negatively impact essential functions

Will the internet still be there, fully intact? The internet was created such that it would be impervious and resilient to *physical* strikes. The master design of the internet allowed for destruction or compromise of substantial portions of interconnecting links without disabling surviving enclaves. In theory those enclaves would then facilitate reconstitution of the physical links. Could wildfire-like, cascading cyberattacks on the internet bring it down? Or can enough internet infrastructure be destroyed to hamper its capabilities? In theory, yes. Practically speaking, probably not. But the difference is immaterial, because the crucial element in connecting or *reconnecting* any network endpoint is mutual trust. If old hardware and systems are lost, new ones must be brought online. Degrading the internet's "white listing" authentication process, the world's insurance of data integrity, could greatly impede attempts at rebuilding internet infrastructure.

While it is unlikely that the internet will be permanently crippled by such an attack, it is highly likely its function would be impaired or degraded for extended periods.

Will "the cloud" survive? The cloud is a massive set of interconnected computers, computer networks, and storage arrays, run by multiple corporate and government entities. The cloud is not a castle in the sky but a terrestrial set of data centers with controlled but "open" access to high-speed communications links. Your organization's "private cloud" may simply be a machine in your own data center. As a technology set, some of the most sophisticated tools available to defend both physical and computing infrastructure protect "the cloud." But it is impossible to know if cloud infrastructure will stand against massive or sophisticated attacks by advanced persistent threats.

The recent year-end report by CrowdStrike, a well-known cybersecurity firm, confirmed that they have seen a growing amount of hacker activity using cloud Application Program Interfaces, known as cloud APIs, the program hooks used by end-user applications to access their cloud functions and cloud data. Data available to a cloud customer is accessed through certain protocols, and those protocols are now the object of intense hacker interest, frenetic testing, and robust exchanges among hacker organizations.

Eliminating part of the internet, or severe degradation or destruction of public or private cloud data infrastructure, is just part of what Greenberg describes as the "thousand such unpredictable outcomes" that could result from a cascading-failure cyberattack. Certainly, major cloud providers have made security a top priority, and the largest companies in the world are pushing cloud technologies. But marketing messages to the contrary, the cloud is just connected, terrestrial infrastructure with many dependencies between a customer and their cloud processing devices or storage arrays, which create vulnerabilities.

Key Takeaway: *Criminal cyber adversaries have morphed into state sponsored adversaries. The threat of financial extortion is real. The threats of cyber war-engendered commercial, financial, and societal chaos are just as real.*

Nation-State Cyber Attacks Will Create Collateral Damage

The goals of cybercriminals are data theft and extortion; the goals of cyberterrorists are chaos and collateral damage that corrode trust, destabilize the social system, and disrupt government. With the rise of nation-state hacking, the system dynamic has changed from data theft and targeted extortion, identifying an entity that can pay ransom to unlock files, to wildly infectious exploits looking to do two things: 1) kill existing systems and 2) propagate to new ones. Stewards of data and technical infrastructure must now assume that any company, group, or enterprise could fall victim to the effects of cyberterrorism, whether they are a specific target or not. When collateral damage is the primary objective, everyone and everything is a potential target.

Imagine the impact of a significant percentage of interdependent technical infrastructure being destroyed in a matter of minutes or hours. A few years before *NotPetya* in Ukraine, Sandworm perpetrated a separate attack that took out the country's power grid. The entire electrical control infrastructure in eastern Ukraine was compromised. Coupled with *NotPetya,* the two damage profiles are massive, and not hypothetical. Effects could include:

- **Electricity:** Electricity grid crippled and cities, homes and businesses in darkness
- **Fuel:** Gas stations unable to pump gas and fuel deliveries disrupted
- **Finance:** Credit card authorizations disrupted, banks unable to honor interbank transfers or local withdrawals, therefore ATMs fail
- **Supply Chains:** Global shipping, port and distribution operations stopped or hampered
- **Food:** Shortages in markets and chaos induced by cash-only transactions and theft
- **Technology:** Computers wiped and rendered useless without rebuild
- **Healthcare:** Medical system disruptions. Hospitals unable to pull up computer records, back-up generators run out of fuel and life support systems fail
- **Telecommunications**: Cell phones and networks fail to connect

The list above is only partial. Damage was both direct and residual. Some results were felt immediately. The longer-term impact developed more slowly, with businesses subsequently calculating real losses in the billions of dollars.

Many of the attack "victims" were likely innocent bystanders. If a nuclear bomb explodes, fallout affects everyone. In a cyberwar, fallout may be random and will extend beyond geopolitical boundaries. Cyberterrorists could undertake a precision strike, but in the interdependent systems of daily life and international commerce, almost everyone connected to the epicenter will be in the fallout zone.

Greenberg in *Sandworm* lays out the details and chronology of these cyberattacks. The compelling thrust of the book is straightforward: The worldwide cyberthreat, and the cyber warfare it is engendering, is not a drill; it is happening now. In the past decade, as a society, some of the drawbacks of technology are clear. Connectivity has led to cybercrime which in turn has now been politically weaponized with a shield of geo-anonymity creating plausible deniability. The hyper-connected world has now made society hyper-vulnerable.

Key Takeaway: *The point of nation-state cyberterror is primary erosion of trust and the costs imputed by collateral damage. We have documented examples of unbridled exploits attacking modern culture at its roots. The threat is not hypothetical. It's real.*

Monolithic Structures Are High-Risk Cyber Targets

Designing computer systems for efficiency and broad deployment has resulted in creating technical systems and technical structures that work with predictable reliability and that have become ubiquitous. This consistency has allowed the connected world to expand with enormous speed along with the growth of ever more useful applications and interconnected systems upon which society has become dependent. Unfortunately, those same repeating technological build patterns have created systemic vulnerability open to cascading system failures. Technological decisions were made for efficiency and in the name of sound design, but they invite trouble in one of two ways: 1) Concentrating data with a high target value. 2) Replicating software that can be attacked repeatedly once a vulnerability is discovered. Engineers optimizing for efficiency have inadvertently created technologically monolithic structures that are now prime targets for cyberattack.

Of the two types of vulnerable monolithic structures in technology, the most obvious are large, physically co-located repositories. Decades ago, management at ESPN (the American sports programming network) decided *not* to place their singular repository of sports media within the World Trade Center in Manhattan. Otherwise that monolith of information and sports history would have been lost in the 9/11 attacks. Instead the vast video library lived in Bristol, Connecticut. Still a singular target, it has since been duplicated to remote facilities to protect against site-specific catastrophic failure as large facilities become natural targets for cybercrime.

The second type of monolithic structure is computer code, copied many times, that can be attacked at each location *the same way*. For efficiency, a company selling popular accounting software in Ukraine used an automated update system. Sandworm compromised that system and used it to spread *NotPetya*. Each company that used the software was a carrier of the virus.

Likewise, the Windows operating system is a monolith. Though not centrally located, it is replicated almost exactly from site to site many millions of times. Once a vulnerability is discovered, it can be exploited again and again at each instance. In addition, the Windows suite of applications, Word, Excel, PowerPoint, are all interconnected with the operating system. Collectively, it is a vast target. Since it is Microsoft's code, they control all the ways data gets into their programs; theoretically they can monitor all the entrances and exits. The challenge for Microsoft is that, as the number of features and enhancements grow, they create new entrances and exits. Unfortunately, as a result, the Windows operating system has been *the* main target of the world's most viral and destructive malware exploits.

From the standpoint of a global threat, it is obvious that each separate Microsoft fortress sits in a web of connected technology. Every operating system makes use of networking protocols— the instruction set that tells data how to move between machines and devices within any given network. The networking protocols were expanded to include the internet, your local computer network's gateway to the rest of the connected world, internetworking with myriad other networks and computers in a large, interdependent, hyper-complex system. The system *as a whole* is the target for nation-state malware, despite the best efforts of the good guys to implement security and to allow only authorized access.

Monolithic structures are prime targets for cyberthreats because one point of infiltration can allow a malign actor to undermine a far-reaching system that triggers multiple dependent ecosystem effects. Farmers have always had a natural inclination against "monoculture"—growing only one crop—for good reason: a single disease or insect infestation can render an entire crop useless. In nature, plants propagate in such a way as to manifest a biodiverse environment that slows plant-to-plant transmission of a virus or other pathogens to which they are susceptible. When crops are planted together, unless they are well protected and properly separated by other species, they are vulnerable to rapid spreading of pathogens. While trees in a forest are independent entities and generally biodiverse, they connect in the "monolith" made up of the air and the leafy canopy. A fire may begin and spread slowly on the forest floor, but its spread at the canopy level can be rapid and capable of "jumping" from one forested area to another if the airgap is insufficient to arrest floating sparks. Through nature and technology, the principle is clear: *Monolithic systems are far more susceptible to attack and subsequent failure than more separated, independent structures.*

For criminals, mugging one tourist may buy dinner, but hitting an improperly secured ATM could have a much larger payoff with less physical risk. For sophisticated criminals, the ratio of risk to reward is best in places that aggregate value. This is especially true when the mechanism employed to commit the crime can access the larger target remotely and anonymously. By extension, while ATM theft may be more lucrative than mugging a tourist, banks provide greater possibilities of reward but also an increased risk of arrest and prosecution. Sociologists have termed this "The Sutton Principle," because bank robber Willie Sutton, when asked by the judge at his sentencing why he always robbed banks, purportedly replied, "Because that's where the money is."

Computing got its start in small, physically and electronically isolated environments. Eventually dedicated hard-wired computers communicated with other equally well-supervised and secured devices. With the advent of the ARPAnet and the accelerant of requirements and funding driven by the Cold War, the communications capabilities and interconnection of computers rapidly multiplied. Their value was limited to military and scientific activities for national defense. While they were of interest to nation-state adversaries, stealing from them was neither easy or of great value.

The advent of the personal computer, including cost-affordable modems and telecommunications, extended ARPAnet-like capabilities to businesses, governments, and eventually, individuals. It also gave rise to the concepts and capabilities that would create the social and economic networks that hold trillions of dollars of value and keys to the national security of many nations. That they share so much in common—interoperable operating systems, hardware, and applications software with compatible metadata and data formats—created a "canopy" through which the "fire" of viruses could travel quickly and efficiently extract value for perpetrators. The modern-day Willie Sutton might say, "Why rob a bank and risk getting caught when you can steal a country's wealth anonymously and get away with it?" His psychopathic sibling might say, "Why burn books in a fifty-five-gallon drum when you can destroy all the information in the world's libraries with a keystroke?"

Cyber criminals and nation-state warriors will continue to target monolithic cyber structures that hold valuable data. To protect against the destructive efforts of cyberterrorism, municipalities and companies will need to invest in decentralized, polylithic systems that dilute the value of any single target.

Key Takeaway: *Our natural tendency to build things for interoperability and efficiency in modular ways has created a build pattern of monolithic technological infrastructure that makes successful cyberterror more likely and more devastating.*

Political and Societal Disruption—Not If, But When

The innate vulnerability of our monolithic systems and the aggressive cyberwar posture of adventuresome nation-states unfortunately makes further cyberterror more likely. There are simply too many variables at play to completely rule out a pervasive cyberattack.

Every day, nation-state actors seem visibly to extend the reach of their malign intent. Making headlines are the cyberthreats that sow chaos through propaganda and misinformation. But Greenberg's sources prove convincingly that Sandworm is undertaking "combined effects warfare," where the propaganda and misinformation teams are working in the same organizations as those teams working to engender chaos and destruction through malware, connected in terms of command and control.

A vigilant defense against the most likely points of cyberattack notwithstanding, the most prudent strategy will focus on after-incident recovery. New attacks are inevitable. Virulent cyberattacks are increasingly common, and there is no reason to think they will stop. Viewed as a gargantuan wrestling match, this cyberwar will have takedowns and reversals. Today cyberthreats are a problem that cannot be fully, categorically solved, only mitigated. With a problem that has no real solution, it is only logical to design systems that lessen the downside effects of attack. Subsequently, while the geopolitical battles of threat and *detente* play out, to sustain data-access continuity, pre-attack vigilance must couple a strategy for after-attack resilience.

According to Greenberg, whose book earns an entire chapter dedicated to "Resilience," the best cybersecurity experts are working worldwide to help prevent the next "cascading security fiasco." Those same experts also know the skill level and commitment of their adversaries, so most acknowledge the inevitability of the next attack. And while they are working feverishly at "lengthening time between failures," they also believe efforts should be made to speed recovery after systems are breached. Organizations that can most readily restore access to compromised data will be the most resilient.

On the same topic, Greenberg interviewed the CEO of the Ukrainian postal service who had experienced the attack of *NotPetya.* "He had no illusions about whether it could happen again." Quoting the CEO: "I don't think we can really prevent something like this . . . We can prepare. And we can try to minimize the damage."

Nobody wants a cyberattack. But assume for a moment that the unthinkable will occur. In that case, it is a matter of personal, business, and national security to take precautions that will make recovery from a cyberattack faster and more likely.

For the average CTO, manager, president, or superintendent, planning for the fallout of cyber war is daunting—the stuff of nightmares. How can regular citizens and entities take responsibility and be prepared for random outcomes of a nation-state cyber conflict? There are some simple principles and practices that are within both the abilities and, importantly, the price range of nearly every organization.

Key Takeaway: *Efforts to prevent cyberattacks may lengthen the time between attacks and attenuate some of the effects. Still, no analyst believes they can be prevented entirely. More alarming to the general public, given the existential importance of an effective retaliatory response to strategic cyberattack, the cloak of secrecy surrounding cyber weapons is such that we have no idea of just how severe an all-out attack could be. Since no absolute solution exists to the reality of cyberwar, after-attack resilience is as important as prevention.*

Creating Resilience After an Attack—Small, Decentralized, Airgapped

Greenberg offers a strategic approach to resilience. “Somehow,” he writes, “societies need to build or maintain backup systems that are disconnected from interdependent, fragile modern networks.” He is arguing for “airgaps”—systems disconnected physically from the rest of the world’s hyper-connected computer networks, a widespread practice in the most sensitive of national security operations in every country on earth.

Although the detailed technical and social consequences of a massive cyberattack may be unpredictable, it is not difficult to understand what will survive:

- Systems that are outside of the targeted monoculture should survive. If it’s an attack on Windows, for example, Linux-based systems should be spared. However, there is nothing to say that a full-scale attack cannot target many types of systems simultaneously.

- Systems (e.g. Windows) that are properly patched against specific sets of virulent exploits should survive. It is critical to keep patches and security updates current against known exploits. However, hackers, especially the best ones, are forever seeking “zero-day” attacks—threats where targeted systems have had zero days to prepare. There is no patch for a “zero-day” attack, because the vulnerability has not yet been exposed.

- Systems and data that have been properly airgapped, i.e. disconnected from the internet and other connected systems, should also survive. In a recent attack, as Greenberg details in *Sandworm*, one company lost over a hundred copies of their critical network routing tables. The *one* copy that survived was on a system in Ghana that had been shut down due to a power cut. It was unintentionally airgapped, but it was airgapped, and the last copy of the needed data survived.

Note: The above scenarios do NOT cover cases of major catastrophic events, physical attacks, or EMP (Electro Magnetic Pulse) blasts. Those problems require solutions that involve multiple, geographically dispersed backup copies.

Of the three survival scenarios above, airgapping is the only one that does *not* depend on luck. Airgapping would include computer systems that are physically disconnected from the internet, where any type of wireless connectivity is also disabled. More extreme airgap protocols would also prohibit the use of corruptible peripherals (CDs/Blu-Ray and DVD disks) and USB storage devices. In addition, all mounting of any storage devices would be controlled and supervised.

The easiest and most straightforward type of airgapping for the general public involves using removable digital storage media—independent devices that can be removed from any type of network connectivity. This category may include USB drives, CD-ROMs and DVDs (optical storage), firewire drives, thumb drives, digital data cards, and especially digital tape.

It is true that all airgapped systems are not the same, and dissimilar categories provide different levels of protection. At the simplest level, USB devices and digital data cards CAN be effective but must be managed carefully. Some "new" external portable devices have circulated where the devices themselves carried malware! In addition, data on many portable devices can be overwritten, therefore they need to be secured between usage. Almost all common forms of portable media are limited in their size and flexibility.

While non-aggregated portable devices are still very useful for small data repositories, digital tape is ideal for large, multi-terabyte or petabyte-scale repositories because it is supported by many vendors offering a wide array of products designed to aggregate data into large airgapped pools. While a network-connected tape library is almost always part of a tape storage system, each individual tape cartridge, if configured properly, *is itself an airgapped fundamental storage unit.*

Providing added protection, digital tape also has the distinct advantage of being "append only," and can be configured such that files, once written, cannot be overwritten in the normal course of operation. The result is that properly configured tape systems can be impervious to after-the-fact encryption efforts. Since each tape is an independent device, protection also extends to efforts to compromise a tape library. The electronic components of a connected tape library could be fried, but the data on the tapes would, under most circumstances, survive.

However, care must also be taken with digital tape depending on the type of protection needed. Single tapes are individually airgapped and offer protection against the main destructive activity of ransomware and other malware. But the physical security of a tape system is also important and is not necessarily protected from sabotage or physical catastrophic failure or attack. Strategies to create duplicate tapes can either take the form of a mirrored system in a secondary site, or most secure of all, duplicated tapes can be physically removed and stored offsite. At a minimum, an airgap is needed. How it is implemented should be thought through by each organization planning their own data security and resilience.

To survive a massive cyberattack, restoration scenarios are needed where critical data can be restored from digital systems that were *not* connected to either local networks or the internet at the time of the attack.

There are really three principles that, if enacted throughout government and industry, could create broad resilience in case of an cyberattack.

1. **Critical backups are distributed and broken away from large monolithic structures**.

2. **Backups exist on airgapped systems or media.**

3. **Each airgapped backup can succeed independently.**

Backups must be verified such that they can restore life to needed systems based on the data on the airgapped systems alone. If the data on a backup is complete and comprehensive, but the indexing and reference system to the backup has been destroyed, the backup data itself may be useless. Data and the metadata used to index and retrieve it are both required for a retrieved backup to be successful. Truly resilient systems must safeguard both necessary components with an airgap.

These three principles, if enacted, can greatly enhance resilience. The approach is not nuanced. The requirement is first to break backup and recovery pods away from large targeted structures, and then to ensure that the major medium of attack cannot harm the separated backup and recovery pods. If the vulnerability is overdependence, make the backup systems independent.

The most virulent cyberattacks cause instantaneous encryption and the disabling of computer infrastructure. Airgaps prevent even the most devious and creative hackers from accessing your data. By making restoration pods local and independent, infrastructure owners and data managers will create local adaptability and resilience.

In no way should this strategy undercut the power and flexibility that online backup systems and cloud infrastructures provide, nor should it blunt initiatives to make cloud infrastructures more secure. However, the best scenario is to *back up the backups* with resilient airgapped pods of data that will speed recovery in the event of a cyber catastrophe.

While government funded programs may underwrite or promote more airgapped repositories, individual organizations *need not wait to make changes.* A small amount of rack space and a modest sum of money per month can secure the data of many organizations from both ransomware and possible destructive cyberattacks. A small business may only need to implement a daily practice of backing up needed data on a thumb drive. Solutions for resilience can be both straightforward and local. The key is to keep data airgapped from any possible destructive attack vectors.

.

To be sure, there will always be threats. The challenge is to diminish the impact of a successful attack, and in the event of a cascading failure, to make recovery faster. Extreme measures and exploits from a committed enemy may succeed. But what will make society far more resilient to a cyberattack is a strategy that creates many separate repositories of data where each is impervious to the main tools of cyberterrorists: i) instantaneous, destructive encryption or deletion of data, and ii) destruction or compromise of the underlying systems that house it.

Key Takeaway: *With resilience and defense as equal priorities, a comprehensive security and disaster recovery strategy will place more focus on creating systems for rapid post-attack recovery. A successful strategy would create backup and recovery pods that are airgapped such that needed data can be redeployed quickly with existing technology as soon as it is safe to do so.*

This is Not A Drill—Virulent Destructive Payloads Are Spreading

When the *NotPetya* virus emerged, it presented as ransomware offering decryption of data for a price. However, *there was no decryption mechanism in the software.* No data, once encrypted with *NotPetya*, was *ever* decrypted. The whole point of the *NotPetya* virus was destruction—nothing more. With *NotPetya* as a harbinger, the news is that every new ransomware or data-theft attack now carries the possibility that it could be part of a plan for pervasive societal disruption.

But why does the public hear so little about this threat?

Victims of cyberattacks—individuals, organizations, companies, schools, and governments—will obscure the details about problems because the targeted entities would rather you not know about their cyber vulnerabilities. Equally, they may be concerned about repercussions and liability. The perverse incentive is to keep things quiet for fear of reputational costs, which subsequently makes it more difficult to warn others of the threat. With estimated ransomware attacks in the *thousands* per month, still nobody wants to claim they have been a target or that their defenses have been breached. Media stonewalling is often officially approved under the banner of "security" to provide time to sort out the cause and remediate or mitigate the damage. As such, companies and organizations say as little as possible after an attack.

The vulnerability to cyberattack is a simple fact of physics—network-attached devices and systems are targets. Criminals and nation-state actors are constantly and aggressively probing for access. The cloud is, in fact, terrestrial and part of all network-attached infrastructure. Wireless solutions are network attached with both hardware transmitters and protocols. In this new war game, the only way to win is to disconnect. The battlefield is networking, computer logic, AI, encryption, "Zero Trust" architectures, and other cyberdefenses—all necessary and commendable. However, airgapping takes data and systems off the field of play. Keeping copies of critical data offline and airgapped is the only way to guarantee their survival in case of a virile, pervasive, destruction-centric cyberattack.

Fortunately, there is no need to wait for national political will to create after-attack resilience. Every consumer, business, government entity, and school or school system, can be proactive about independently protecting their critical data from attack. Nobody needs permission to airgap critical recovery data. Airgapped recovery systems for small businesses and government entities can be deployed for a few dollars a day. Larger airgapped systems can be fully automated and made transparent to any existing operations.

Key Takeaway: *With a "not if, but when" approach to cybersecurity, a simple conversation about how to recover from cyberattack is in the interest of literally every business, school, and public sector entity.*

Conclusion

There is an undeclared hot war underway. Unfortunately, normal citizens and organizations from anywhere may be affected. Those responsible for the safekeeping of data are directly in the crosshairs of both criminals and nation-states. Yet, unlike other wars, tools and technologies exist for any group to enhance the possibility of after-attack resilience. Data repositories large and small can be broken up and then airgapped for maximum resilience.

Every internet connected device today is a potential point of attack from cyberterrorists. Large, monolithic systems are prime targets. Approaches and technologies exist that make it possible for an organization of any size to mitigate the damage and to rebound seamlessly after an attack. The reality of the threat, and its solution, are obvious. The wise will acknowledge the threat, invest in resilience, and plan accordingly.

Authors Note, January 2021

In December 2021, US intelligence agencies uncovered a cyberattack perpetrated by Russian hackers, the very group described in *Sandworm*. This was a real-world, nation-state attack. The damage is unknown or has not been revealed. The depth of the attack is understood to be broad, carried to the agencies in a commercial software update – like the malware vector of *NotPetya.* The threat to worldwide systems via nation state attack is not theoretical. This further escalation of the present cyber war has begun.

About the authors:

Fred Bonner is a technologist and a founder and CTO of EchoLeaf Systems. He is a graduate of Duke University with a graduate degree from the University of Maryland in Management of Technology. His professional career has been spent at BellSouth, The Discovery Channel, IBM, Imagine Communications, and EchoLeaf Systems. His specialty is the virtualization of removable digital storage media and the management of large data archives.

Peter Guglielmino is an IBM Distinguished Engineer. He has worldwide responsibility as CTO for IBM's Media & Entertainment Industry. He is a graduate of Oneonta State College in NY. Among his many specialty concentrations are Hybrid Data Management and Data as a Service.

R. David Henze-Gongola is a former U.S. Navy Cryptologic Technician, an IT executive, and Senior Advisor to several high-technology companies at Henze Communications, LLC. He has provided technical, operational, and program management support to the U.S national security and law enforcement communities and global financial companies. He graduated from George Mason University with a BIS degree in Russian Strategic Studies, and he earned his graduate certification in Electronic Business from George Washington University. Time allowing, he has supported the NY Electronic Crimes Task Force as an industry volunteer since 1997.