New Cyber Threats Demand New Solutions

Fred Bonner
CTO EchoLeaf Systems
September 2022

Introduction:

I was the first IT Director at The Discovery Channel, and later spent over a decade with IBM working in data and data protection. I have dedicated my career to the management and protection of data and digital assets.

Unfortunately for the world, the concept of data protection now requires a paradigm shift. This shift has been necessitated by the sophistication and skill of the world's cyber criminals, and the enormous resources being spent by nation states to gain technical and political advantages over other nation states. Full disclosure, I have chosen to be in the business of working on this problem. However, three central truths have emerged that are critical for anyone managing data to understand. I feel compelled to articulate them – and I urge an industry-wide conversation about how best to achieve the goals of data protection given the new realities.

1. Bad News -- Your Connected Data Is Inherently Insecure

ANY connected data – data that lives on a network or connected cellular device – is inherently insecure if attacked by a committed enemy. If there are *ever* live connections to the data, somebody can get to it. This includes data on your cell phones, data in the "cloud" (basically somebody else's wired data center,) on premise at work, or in your home. The monumental effort to find "Zero Day" exploits – holes in data systems that vendors don't know about – and the global market for those exploits, have made it so that no code or system is completely secure. In almost every computer network holes and exploits abound, and it is literally impossible for any group to say, with certainty, that their *connected* data is 100% safe.

A few smart people have written in depth about the acute nature of today's cyber threats, and I consider these books essential reading for data professionals or anyone who feels that protecting data, of any sort, is part of their remit: *New York Times* reporter Nicole Perlroth's book *This Is How They Tell Me the World Ends.* (Bloomsbury Publishing, 2020). Slightly shorter but no less frightening, Andy Greenberg (Wired) wrote *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. (Doubleday, 2019).*

One of Perlroth's chilling conclusions, paraphrasing a world-renowned cyber expert -- there are as many vulnerabilities as there are stars in the sky. The main vendors selling cloud and data protection services don't know what they don't know because Zero Day exploits are, by definition, only known to those who have discovered them.

There is no happy ending to this story. In terms of “enemies” we are talking about sophisticated, numerous (10s of thousands at least) committed, heavily funded hackers using extremely advanced tools. Big print in vendor ads will tell you your data is safe. The small print in the contract will remind you otherwise. If your information and data is “connected” – on a network, in a data center with outside connections, or on any type of wireless device – no-one can *guarantee* the safety of your data.

Your data can be a target of theft. Or your data can be in the blast radius of a larger attack and destroyed, literally, without warning. If your data is connected, there is nowhere to hide. This is the truth – for connected data.

2. Build Resilience by Expecting (and Planning For) a Major Breach and Loss of Data

As vulnerable as they are, connected systems are the lifeblood of modern computing. Our world IS online and connected as a practical matter. But given the realities of the vulnerability of all connected systems, data managers must be prepared if/when those systems are destroyed or compromised.

Present defensive efforts to protect data against known risks are essential, of course. We need perimeter defenses, endpoint defenses, sniffers, education, various end-to-end encryption schemes -- and others too numerous to mention. Some risk can be transferred with outsourced IT, cloud implementations, and cybersecurity insurance (if you can afford it.) But after a breach, transferred risk might get you a refund on service costs, an apology letter, or funds to help rebuild compromised or disabled systems. It cannot restore either your company’s reputation or data that has truly been lost.

“Disaster recovery” has long been an essential part of IT. But a natural disaster is far different than a disaster caused by malicious actors. “Normal” backups got us through normal disasters. A more advanced paradigm for data protection is essential for recovery from a malicious breach.

Rather than being shocked by malicious attacks, acceptance and preparation of the new risk is required. As Perlroth states: “In truth, there is no one running point” to solve the problem of runaway Zero Day exploits and their consequences. Our government is as busy as any other adversary finding and stock-piling Zero-Days that might be needed for defense or attack. *Only a few are shared with vendors.* History has shown us that some of those exploits can get into the wrong hands -- with catastrophic results. The most notorious example is that the United State’s attack on Iranian nuclear centrifuges, after it was discovered, was reverse engineered, and pieces of THAT exploit (*the Stuxnet worm*) were found in the subsequent *NotPetya* attack that affected global supply chains.

To counter threats successfully continuous improvements will be needed to keep up with the bad guys, along with periodic tests, audits, and drills as threats change. Most importantly, we cannot be surprised when these efforts fail and system restoration is required. The Titanic was theoretically unsinkable. It still had life-boats.

The good news? Restoration after a catastrophic cyber breach is possible – with the proper planning.

3. Multiple and Enhanced Strategies Are Required for Both Defense and Complete Restoration

System admins can counter attacks on connected systems by creating *unconnected* pods of data that are beyond the reach of cyber threats. Unfortunately, for true system *restoration* after a breach, the phrase "back up your data" is insufficient given the level of possible attacks.

To protect your data, it MUST be airgapped at a minimum. Literally there must be air between all connected systems and your data, on devices with no wired or wireless connections. However, in the new paradigm for safety, *airgapping* is only the first step. Why? Because when creating backup sets, malware can be obscured within "good" files. A corrupt file, backed up and airgapped, is still a corrupt file.

In addition to airgapping, secure data should be in a read-only medium such that good files cannot later be overwritten. Read-only data – like that on append-only data tape – prevents good files from turning into bad (encrypted) files – the favorite trick of ransomware attackers. It is essential that data used to restore compromised systems has not itself been corrupted. Read-only media helps to accomplish that level of protection. In addition, when data is restored after a breach, it may need to be examined first. Therefore, a safe place to perform forensic analysis will be required..

Data copies should also be encrypted – since *if* they are somehow stolen, they should be rendered useless to thieves.

For added protection, airgapped, read-only, encrypted data should be in a medium where egress can only be achieved through "spooling" – moving out only a string of 1's and 0's at a time, rather than with a mass move of ALL your data. Why is this important? Because data spooling makes it far easier to implement egress alarms that can warn you if unauthorized parties are moving too much data at once.

More bad news, almost all data encrypted with the industry standard AES 256 encryption (the highest industry standard) will be obsolete in less than a decade. Quantum computers will be able to crack it – and they are being developed faster than expected. So be ready to re-encrypt your AES 256 encrypted data with Post Quantum encryption -- which does exist. Obsolete encryption is an unavoidable problem. Re-encryption to new standards *will* be required.

Intelligently organized digital tape systems can deliver all the above requirements today for rapid restoration after an attack. But to be clear, where once the simple airgap was enough, today's advanced hackers require that your data is:

- airgapped
- on a system designed for forensic analysis
- on a read-only medium
- encrypted (post-quantum encryption recommended)
- with "spooled" egress and egress alarms
- AND easily accessible to authorized users

The recommendations above help organizations adhere to the latest Zero Trust Architecture principles, while allowing rapid, timely restoration of critical systems after a system breach.

Summary and Conclusions:

Connected data is not safe. Unknown exploits abound, and by their very nature it is impossible to protect against all of them.

Good planning dictates creating resilience plans that can be implemented quickly and efficiently. Addressing a “worst case” breach today is far more likely than it was even a few years ago.

Defenses are essential and required. Security tools today have been created to protect against KNOWN threats. The evolution in our thinking is also to protect against UNKNOWN threats. NIST has developed recommendations for securing storage (NIST SP 800-209 Security Guidelines for Storage Infrastructure) which include ZTA, airgapping, read-only copies, forensic analysis, rapid restoration, and encryption. All of these technologies are available and required to meet the newest security threats of today.

A whitepaper detailing a specific storage architecture cross referenced with NIST SP 800-209 is also available here. (Compartmentalized Cyber Security and Incident Recovery)

Fred Bonner is a founder and CTO of EchoLeaf Systems (www.echoleafsystems.com)