Cyber Protection at Home

by Ken Clipperton, DCIG Lead Analyst, Storage

Cyber protection at home has become an important consideration for businesses of all sizes. This article reflects what I learned from the recent failure of my primary home office computer.

Acronis

COMPANY

Acronis
1 Van de Graaff Drive,
Burlington, MA 01803
+1 (781) 782-9000

www.acronis.com

INDUSTRY

Cyber Protection

CHALLENGE

- With so many businesses now urging or requiring employees to work from home, cyber resilience at home has become an important consideration for businesses of all sizes.

SOLUTION

- Acronis True Image for Individuals
- Acronis Cyber Protect for Businesses

BENEFITS

- Anti-ransomware and anti-malware protection
- On-site and off-site backups
- Full-image backup and restore

Cyber Protection at Home

DCIG focuses its research primarily on enterprise storage and data protection. This article is, and is not, a departure from that focus. With so many businesses now urging or requiring employees to work from home, cyber resilience at home has become an important consideration for businesses of all sizes. I routinely work from home and recently experienced the failure of my primary work computer. This article reflects what I learned about cyber protection and resilience at home from that experience.

Taking Our Own Cyber Resilience Advice

In March 2020, Jerome Wendt published a gripping article called *An Anatomy of Responding to and Surviving a Ransomware Attack.* He based the article on an interview of the COO at a large professional services firm that believed it was well-prepared to respond to any natural disaster or attack; yet discovered it was still vulnerable. Jerome closed the article with this statement, "It is the hope of DCIG and the firm that readers of this content will become more aware of the threat that ransomware poses and take the appropriate actions to protect themselves from it."

After discussing the article with Jerome, I decided to take a fresh look at my own level of cyber protection at home. I am glad that I did.

An Ounce of Cyber Protection

As an analyst for DCIG, I routinely work from home. My technology setup includes a home firewall appliance that sits between my Internet router and the networked devices in my home. I run a well-regarded Internet security suite on all the computers in my home. I use one of the popular services that keeps a copy of my documents in the cloud.

Nevertheless, in light of the ransomware threat, I decided to add another layer of protection. After reviewing multiple alternatives and trying out the two most promising packages, I selected Acronis True Image for its anti-ransomware, on-site and off-site backups, and full-image backup and restore capabilities.

Failure

The motherboard of my primary work computer failed a week after I began using Acronis True Image. The computer was under warranty, and I had purchased an extended "next-business-day on-site after remote diagnosis" support agreement, so I was covered. After several hours on the phone with the technical support department, we determined that in the process of failing, the motherboard had killed both the boot SSD and the data HDD in the computer. Rats!

> ***"After reviewing multiple alternatives and trying out the two most promising packages, I selected Acronis True Image for its anti-ransomware, on-site and off-site backups, and full-image backup and restore capabilities."***
>
> **— Ken Clipperton, DCIG Lead Analyst, Storage**

At this point, I was very glad that I had created an Acronis Survival Kit backup of the entire computer just a few days prior to the failure.

Discovery—NBD On-site Does Not Mean Tomorrow

The computer failed on a Saturday. The support technician told me that the parts I needed would ship on Monday, and a tech would be on-site on Tuesday. I did not receive a shipment notification Monday morning, so I checked in with support. I learned that the vendor did not have the boot SSD in stock. They expected to receive the part the following Tuesday. I could expect to see a technician Wednesday or Thursday of that week—ten days out!

The on-site technician told me that they had started seeing delays in January, shortly after the news about the novel coronavirus began to spread. She indicated that these delays were increasingly common. She also mentioned that her husband had recently been required to begin working from home. He had found it challenging to locate the furnishings and supplies he needed in order to set up a functional office at home.

A Bird in the Hand—The Value of On-site Spares

As a former IT director, I knew the value of on-site spares in accelerating recovery from failure. I keep two older, but still functional, computers on hand and routinely boot them up so that they receive operating system and other software updates. I also run the file synchronization service on these computers, so they have local copies of my work documents. Thus, after my primary work computer failed, I switched over to using a spare computer with minimal disruption.

Speeding up Recovery

The onsite technician repaired the computer and installed a base Windows image. The computer booted but did not yet have my software or documents. I used the Acronis Survival Kit to rapidly rebuild the data disk. However, restoring the boot disk was going to require extra steps due to the motherboard having been replaced. After several chat sessions with the system vendor and Acronis technical support, I determined it would be quicker to start from the base Windows image and then re-install my software.

Several items I had on hand helped to speed up the recovery process. I recommend these for everyone's cyber resiliency kit. These include:

- Windows boot media
- A System Recovery Disk
- An external HDD to hold a local copy of backups. This enables faster transfer of files to the repaired computer than can probably be achieved across the Internet.
- A "software downloads" folder on the external HDD with copies of all the software that you installed on the computer.
- A password manager that securely stores passwords for all the software and services that you use.

Cyber Resilience at Home

Businesses that have had work-from-home options in place for a long time also have policies and guidance for establishing a functional and cyber-resilient home office. For those businesses that are new to work-from-home due to the COVID-19 pandemic, I hope that my recent experience will suggest some steps you can take even now to increase the cyber resilience of your home office.

Cyber Protection for the Enterprise

Acronis True Image is the company's consumer/prosumer product. Organizations that are needing to centrally-manage cyber protection—especially given the surge in its remote workforce—should take a look at Acronis Cyber Protect Cloud service available through managed service providers.

This product is an AI-enhanced solution that integrates data protection with cybersecurity, empowering enterprises and service providers with prevention, detection, response, recovery, and forensic capabilities.

The product is enriched with next-generation, full-stack anti-malware and anti-ransomware protection and comprehensive endpoint management tools like patch management, vulnerability assessment, and remote management. Built on top of Acronis' highly-regarded backup and disaster recovery solution, Acronis Cyber Protect Cloud simplifies onboarding, daily operations, and reporting while combating advanced attacks.

Additionally, Acronis is rapidly rolling out the following features in the product in response to the COVID-19 pandemic such as:

- ***Easy Remote Desktop access from Windows or Mac.*** When Cyber Protection Console is used on a Mac, it can launch RDP client from the management console, same like on Windows to add more flexibility for Mac-based admin.
- ***Acronis VPN for Increased security.*** MSP will install VPN appliance in the corporate network and initiate disaster recovery scenario. Thus, remote workers will have access to the corporate network via L2 VPN.
- ***Special protection plan for remote workers.*** Predefined protection plans for office and remote workers—with more strict options (more frequent backups, "deny all" option for Active Protection and URL filtering, Battery).
- ***URL filtering that protects from Covid-19 scams.*** Block Covid-19 fake news, malicious and phishing sites by Acronis URL filtering. Database of such URLs will be updated regularly and promptly.
- ***Mission critical telecommute apps priority patching.*** Popular collaboration and VPN apps added into VA/PM database to provide additional security: Zoom, Teams, Skype, WebEx, Slack, TeamViewer and dozen popular VPN clients.

- ***Easy remote Windows-based machine wipe.***
  Situation may require to remotely wipe Windows-based machine. Ad can easily initiate this operation from Acronis Cyber Protect management console.
- ***Additional CPOC alerts related to public health.***
  CPOC alerts related to Covid-19 news, viruses and potential outbreaks, including epidemic, pandemic, another viruses outbreak or themed malware
- ***Keep germs away via voice controlled Cyber Console.***
  Support for Touch-less UI to assess functionality of Cyber Protect Console by voice to improve productivity and minimize contact with potentially contaminated equipment.
- ***Remote Desktop connectivity for the end-users.***
  Remote workings need to establish RDP connection to the office computers. Admin will be able to share remote access link to a specific machine with a user requesting it.

Act in Haste or Repent at Leisure

The current cyber threat environment turns the adage, "act in haste, repent at leisure" on its head. Ransomware and malware attacks are increasingly common and shockingly successful. The sudden transition to working from home due to the COVID-19 pandemic has created a substantial new attack vector, especially for companies that do not have a well-established work from home program. Now is the time to implement cyber protection that extends to the home offices of all an organization's employees. ■

About Acronis

*Acronis leads the world in **cyber protection**—solving safety, accessibility, privacy, authenticity, and security (SAPAS) challenges with innovative **backup**, **security**, **disaster recovery**, and **enterprise file sync and share solutions** that run in **hybrid cloud environments**: on-premises, in the cloud, or at the edge. Enhanced by **AI technologies** and **blockchain-based data authentication**, Acronis protects all data, in any environment, including physical, virtual, cloud, mobile workloads and applications.*

*With 500,000 business customers, and a powerful worldwide community of Acronis API-enabled service providers, resellers and ISV partners, Acronis is trusted by 100% of Fortune 1000 companies and has over 5 million customers. With dual headquarters in Switzerland and Singapore, Acronis is a global organization with offices worldwide and customers and partners in over 150 countries. Learn more at **acronis.com**.*