TechTarget | Custom Media

How the Role of Backups Has Changed in the Ransomware Era

The role of backups has changed in the modern era. As attackers get smarter and more focused, IT managers have to change with the times as well. Attackers are getting more adept at penetrating networks, necessitating that backups become more sophisticated and cover a multitude of circumstances, threat models and conditions. And as we change the way we work, the way we consume data, the way we build our business computing systems and the way we depend on more complex online systems, we need to change the way we make backups, too.

Sponsored by
Veeam Software

April 2018

First off are the **very different working conditions experienced by most businesses today versus a decade ago**. Employees are now spread all over the globe, and many people are working from home or smaller remote office locations. Almost everyone is using their smartphone for business functions and creating data that resides only on their phones. And people are working more hours in the day, so the old notion of doing backups in off hours is somewhat quaint. "Work used to be somewhere you went during the day. Today's users are placing new demands, and their data needs to be available 24/7, from wherever they might be located," says Ken Pipkins, a cybersecurity account manager at Cisco Systems.

These trends place more demands on ensuring that business data can be located and then backed up properly. "You need to understand where your data resides and how it is critical to your business, and also know how quickly it can be restored," says Rick Vanover, director of product strategy at Veeam Software. "That means there is more of a digital dependence in the average business, because you need both visibility and resiliency in your backups."

The **way we build our computing systems has also changed** in the past decade. Older backup tools weren't specifically designed for today's heavily virtualized environments, which means that backups can't easily scale for growth in accessibility and the increasing volume of data stored by today's companies.

"While there are still many hardware-centric applications out there, most corporations are using more virtual servers to leverage their hardware investments better," says Pipkins. "This has created a challenge for enterprise backups. The nature of how users consume and create data has changed drastically in the past decade," says Ryan Lally, a security sales specialist at World Wide Technology.

But it isn't just virtualization that has changed how we build our systems. **Most businesses today have some online footprint**, and that presence is increasing as more software moves to the cloud and is being used on an as-needed basis. This places more of a demand on recovery times to bring a backup back online quickly. "That has led to unreliable backups, too-long recovery periods, challenges in meeting compliance requirements and a lack of ability to scale backups. As we see more growth in accessibility and the amount of data that we have seen being stored by these companies, you have to redesign your backup solutions," Pipkins says.

The expansion of our geographic reach means the potential for cyberexploits expands as well.

"Organizations aren't doing enough for disaster recovery and need more than simple backups," says Vanover. "They often fall far short of the total recovery experience and need to develop their strategies more completely to protect them from today's threats."

The expansion of our geographic reach means **the potential for cyberexploits expands as well**. This changes the mix of potential threats, which can be an issue for companies that are still stuck in the past. "Back then, no one had yet heard of ransomware. Now, it is in the news every day," says Pipkins. "And there is more of a threat coming from the Internet of Things and connected devices on power grids or shop floors. It is a lot harder to protect these areas."

What some companies have done is to give in and pay the ransom demands, which can be an issue because there isn't any guarantee that they can decrypt their data across all the affected systems or that their business won't be disrupted for days or even months.

Another consequence of these expanding threats is that **backups need to be just one part of an overall defense-in-depth strategy** that covers many different protective layers. "You have to assume that eventually you will fall victim to a ransomware or some other malware attack," says Lally.

While these circumstances show how different today's computing environment is, there are some things that haven't changed much since the very early days of PCs. "There is still a massive amount of malware coming in over web and email paths, and these are still the easiest ways for a corporation to get infected," says Lally. "The result is that the endpoint is still the biggest source of threats. And with tablets and the cloud, there are massive blind spots in your security. Attackers are always trying to find administrative accounts and passwords because that gives them the greatest flexibility in their attacks. We often see that many enterprises don't know how many administrative users they have or let developers have full access to network resources but don't really track whether they really need this or not." Sadly, that statement could have been true back in the 1980s.

Email security actually went out of fashion for a while but has come back, according to Pipkins. "We are seeing a resurgence in email attacks, particularly for spear phishing, where email has once again become an attack vector by taking fraudulent websites and embedding them in email messages," he says.

Another consequence of these expanding threats is that backups need to be just one part of an overall defense-in-depth strategy that covers many different protective layers.

"While a percentage of phishing attacks can be thwarted with education and security awareness, that isn't enough, and customers need good email security technologies in place to really protect their users," says Lally. "Many enterprises are using technologies such as DMARC [Domain-based Message Authentication, Reporting and Conformance] to try to make email spoofing more difficult and easier to detect. But ultimately, you have to harden your email attack surface." He also recommends people use multifactor authentication, single sign-on and step-up authentication to protect themselves against malware. "You need to understand the individual use cases and potential threats, and also consider how remote users access your networks," he says.

Finally, another thing that hasn't changed much over the years: **verifying backups**. Often corporations find out the inadequacies of their backups only after they have been hit by an attack and can't easily restore their systems or recover all of their data. "If you don't have good backups, shame on you," says Lally. "An enterprise should be able to withstand a ransomware attack, but I have seen many of them lose millions of dollars in intellectual property because it wasn't ever backed up properly, or because they had operational issues after the attack."