White Paper

Addressing Cyber Protection and Data Protection Holistically

Sponsored by: Acronis

Phil Goodwin Andrew Smith Robyn Westervelt

June 2019

IDC OPINION

Cybersecurity threats are among the highest concerns of IT managers and organizational executives alike because security incidents and data breaches can result in reputational loss, direct economic loss, and regulatory sanctions. IDC research shows that 93% of organizations have been attacked within the past three years — and we believe, tongue in cheek, that the other 7% of organizations are simply unaware of it. Moreover, nearly half of organizations have suffered at least one unrecoverable data event within the past three years.

Cybersecurity risk notwithstanding, IDC estimates that 60% of organizations will have a digital transformation (DX) strategy implementation in progress within the next 24 months. DX initiatives are seen as critical projects to improving the competitiveness of the organization by feeding faster, more accurate decision information to business leaders. Our research shows that data availability is a key factor in more than half of IT transformation (ITX) projects and consumes about one-third of the ITX budget.

IT transformation is a key component of a DX strategy, and data security and availability are cornerstones of ITX. However, managing data protection across increasingly hybrid environments is becoming more complex as threats become more diverse and sophisticated. Moreover, the nature of DX — distributing and collecting data from diverse systems and geographies — reduces visibility and control of the data for IT staff. According to IDC research, data security, ensuring data quality, the shortage of skilled security professional, and regulatory compliance are the most significant challenges cited by IT professionals. Among those we surveyed, 40% cited sophistication of attacks and complexity of security as the greatest challenges.

Data availability and security are foundational to ITX and therefore DX. Effective use of data results in improved operational efficiencies and organizational performance, but IT teams need to elevate and enhance their cybersecurity strategies accordingly. Cyber protection — defined as the convergence of data protection and cybersecurity — is a key to mitigating risk.

IDC recommends that IT organizations take the following actions:

1. Create a cyber protection center of excellence that focuses on data security and availability in ITX operations.
2. Embrace a strategy of cyber protection by more closely integrating data protection, disaster recovery, and data security operations.
3. Design cyber protection into infrastructure architectures, not as an add-on.
4. Leverage automation and artificial intelligence (AI)/machine learning to maximize responses to evolving threats.

SITUATION OVERVIEW

No one is immune to cyberattacks, whether corporation, governmental agency, or individual. Attack sophistication is constantly evolving and improving: it is a veritable arms race between the good guys and the bad guys. These attacks may be attempts at gaining sensitive information such as personal identities, account credentials, and credit data. There may also be attempts at corporate sabotage or espionage. Importantly, the onslaught of ransomware cases demonstrates that attackers are increasingly likely to hold data hostage by encrypting it and extorting financial payments to attain the return of the keys for decryption.

While the IT environment is becoming more complex, cybercriminals are getting better at identifying and targeting these intrinsic weaknesses. Nearly 40% of IT security, line-of-business, and data management specialists cited the rising sophistication of attacks and the increasing complexity of managing and supporting security products as significant challenges, according to IDC's *Data Services for Hybrid Cloud Survey.* Attackers benefit from complexity, which may lead to configuration weaknesses and user ignorance. With the increasing attack surface across on-premises infrastructure, cloud infrastructure (public, private, and multicloud), and endpoint devices, the number of potential vulnerabilities is growing as well. Continued cloud adoption and data migration projects have enterprises of all sizes reassessing their security strategies after uncovering gaps in coverage. The survey data suggests that bolstering data security and mitigating cloud risks will require not only technology but people and process changes as well.

Cybersecurity has been an IT discipline for more than two decades, but cyber protection is quickly becoming an IT discipline in its own right. It enlists the skills of traditional backup/recovery, disaster recovery, cybersecurity, and storage management specialists to support the organization's data security strategy. These professionals must assess and modernize backup and recovery plans and address system redundancy and failover.

Both cybersecurity and cyber protection functions must be coordinated into a continuum of protection that bridges their traditional silos. These newly integrated functions must be regularly assessed to ensure adequate enforcement mechanisms to defend against fast-evolving threats like ransomware, which increasingly demand sophisticated software capable of dynamically adjusting to new strains as they emerge.

In addition to the reputation damage, direct and opportunity costs, and regulatory sanctions mentioned previously, cyberattacks can result in unplanned downtime, loss of competitive trade secrets, and permanent data loss. IDC research has found that the average cost of downtime industrywide is $250,000 per hour. Comparing the cost of attack prevention and recovery software with even one hour of downtime often justifies the cost. In many cases, breaches now require public disclosure, ensuring reputational damage that is often long lasting, with no way to repair permanently lost customers or data. IDC research has found that reputational damage occurs in almost half of data breach situations, further increasing costs and justifying the costs of recovery.

Much has changed from the early days of computing when hardware error, software error, and human error were the main causes of outages and data losses. Those scenarios have been largely alleviated with more reliable hardware, redundancy, and automation. Today, the major threat to data is cyberattack. Fortunately, the industry is responding with new products and technology to help organizations address this risk.

FUTURE OUTLOOK

IT organizations are rapidly rising to the challenge of cybersecurity and cyber protection. More than half of organizations we surveyed have established a team tasked with ensuring business resilience. Almost a quarter of them have built integrated IT and business unit teams around business resilience. Nevertheless, many find themselves behind the curve of evolving threats because they are relying on older technologies and methods that bad actors have already learned to thwart, such as signature-based antivirus.

Cyber protection tools may be separate or integrated with threat detection software. These components include backup, offsite disaster recovery, malware detection and protection, intrusion detection, encryption and authentication, and secure tiered storage, including offsite and/or cloud capability. Of course, the solution is not just technology — people and processes also play important roles. Often, it is the processes that bring each component into a coordinated whole and the people who keep the processes current and functioning while needing to identify and defend against attacks leveraging social engineering.

Certain new, emerging technologies are becoming key to cyber protection. These may deploy AI and machine learning techniques to spot the anomalous behavior that often precedes an attack. They also may involve cloud deployments to enable scale, speed of deployment, flexibility, data separation, and physical security. We believe that AI is essential to successful cyber protection. Systems must be able to detect zero-day attacks: dangerous exploits that have not previously been encountered, where waiting for a known threat signature is ineffective.

The growing prevalence of data storage and backup archiving in the cloud, alongside the parallel rise in malware attacks on data integrity, is contributing to the increased importance of scalable means to ensure and publicly attest to data integrity. Companies, their customers, their business partners, and other actors (e.g., parties in lawsuits pursuing ediscovery) increasingly need proof that data, regardless of the repository in which it has been stored or backed up (e.g., in public or private clouds), has not been tampered with, and that what was stored or backed up and what was recalled from storage or backup is identical. Blockchain technology is emerging as an effective technology for ensuring data authenticity.

We believe that AI (for behavioral detection and termination of cyberthreats) and blockchain (to ensure and attest to data authenticity) will be the two key components that IT organizations will look for in cyber protection products.

Technology by itself cannot comprehensively mitigate these risks. The current shortage of skilled security professionals also requires people and process changes. The newly adopted security and data protection technologies need to be proactively maintained; existing security solutions often need to be reconfigured or replaced to effectively address security risks across hybrid environments. IDC survey data found that operations, line-of-business IT, and IT security practitioners are in agreement that the already heavy burden of security and compliance tools and activities can be worsened by the increasingly distributed nature of data and the accompanying need to manage hybrid cloud data services. An integrated, holistic solution provides simplicity in the face of this growing complexity. It ensures a common user experience and provides across the board functionality that can significantly reduce the management burden.

Considering Acronis

Acronis is among the tech vendors at the forefront of developing cyber protection solutions that integrate data protection and cybersecurity capabilities. The Acronis cyber protection platform includes a worldwide network of cloud datacenters capable of offering backup as a service (BaaS) for customers and service provider partners as well as on-premises backup. This solution is designed to cover servers, virtual machines, traditional applications, cloud-native applications, edge and mobile devices, and any combination thereof. This can include hybrid cloud (on-premises to public cloud) as well as multicloud (public to public cloud). This broad architectural coverage helps ensure that an entire environment is under the Acronis cyber protection umbrella. Acronis describes its cyber protection strategy as being based on five vectors:

1. **Safety –** A reliable copy of the data is always available.
2. **Accessibility –** Protected data is available anywhere, anytime.
3. **Privacy –** Access to and visibility of data is restricted to authorized parties.
4. **Authenticity –** Data copies can be proven to be exact replicas of the originals.
5. **Security –** Data is protected against threats and malicious agents.

Acronis integrates its so-called "five vectors of SAPAS" across its product lineup as follows:

- For increased data safety, Acronis implements a hybrid data storage model designed to allow customers to leverage any data destination: local disks, tape, Acronis Cyber Infrastructure (a hyperconverged storage appliance), and any cloud (including Acronis Cloud Storage as well as public cloud storage from Google, Microsoft, Amazon, and other service providers' cloud storage offerings).
- To improve accessibility of the data, Acronis implements granular recovery with Acronis Universal Restore, which is designed to make recovered data available in seconds or minutes. Backups can be recovered to a dissimilar environment to speed up the restoration process: physical to cloud, virtual to physical, or any combination. Acronis also allows secure web access and the ability to search through cloud backups, enabling quick discover and access to any data.
- To ensure data privacy, Acronis combines policy management, encryption in flight and at rest, group policy administrators, and tenant isolation to form a comprehensive data privacy policy.
- Acronis Cyber Notary and Acronis Cyber Notary Cloud are blockchain-based services for file notarization, esigning, and verification for businesses of any size to ensure data authenticity.
- Acronis Active Protection is an advanced AI-based technology that is designed to ensure the security of data processing environments by automatically detecting and terminating ransomware attacks and other malware incursions like cryptojackers while simultaneously and immediately restoring any encrypted files from backup.

These capabilities are integrated across the entire Acronis product lineup, including:

- **Acronis Cyber Protect** is designed to be a full-stack antimalware protection and comprehensive endpoint management solution integrated with advanced backup capabilities, patch management, vulnerability assessments, and AI-powered hard drive failure detection.
- **Acronis Cyber Infrastructure** (software-defined infrastructure) is designed for corporate customers and managed service providers to access the reliability, cost efficiencies and universality of software-defined, multipurpose infrastructure.
- **Acronis Cyber Platform** is an ISV toolkit to support the development of a broad range of data protection services using APIs and SDKs for customization and integration into the core Acronis cyber protection technologies.

- **Acronis Cyber Cloud** is a multitenant cyber protection solution designed for both private cloud and managed service provider deployments.
- **Acronis Cyber Notary** is a blockchain-based service for file notarization, signing, and verification. The related **Acronis Cyber Notary Cloud** offering is designed exclusively for service providers to use as a platform for offering blockchain-based data authentication as a service.
- **Acronis Cyber Backup** is the vendor's core backup and recovery product for physical and virtual workloads, endpoints, and structured and unstructured data whether on-premises, in the cloud, or in hybrid clouds.
- **Acronis Cyber Disaster Recovery** is the vendor's disaster recovery-as-a-service (DRaaS) solution and includes disaster recovery orchestration, runbooks, and failover testing.
- **Acronis Cyber Files Advanced and Acronis Cyber Files Cloud** is a secure corporate file sync and share solution for both corporate customers and a private label or co-branded option is also available for managed service providers.

In summary, Acronis has designed its solutions to offer IT organizations better control of their cyber protection environment through global policies, role-based data management, and encryption. Security is enhanced using active AI-based ransomware detection, alerting, and automated recovery with certified data authenticity. Finally, the product architecture is designed for universal scale-out deployment with simple implementations and management.

CHALLENGES/OPPORTUNITIES

Cyber protection is a rapidly emerging market filled with myths, misperceptions, and unknowns. As a relatively new vendor to this space (albeit from a strong data protection background), Acronis will be challenged to make its market message heard in a cacophonous marketplace and to educate IT professionals on the topic. AI is an emerging technology and will take considerable resources to keep in the arms race with bad actors, who will keep countering with their own AI-enabled malware. Every vendor in the market, including Acronis, must recognize that it cannot do everything: partnerships for key technologies and capabilities will be essential for a truly complete solution.

CONCLUSION

We believe that the emerging integration of data protection and cybersecurity into the new discipline of cyber protection will play an important role in the success of DX initiatives. Growth of malware sophistication, ransomware, and targeted attacks is multiplying the major threats to data availability and accuracy, so taking stock of existing defenses and processes is paramount. This imperative is supported by IDC survey data: Identifying data quality issues and ensuring data quality was cited second highest (behind data loss prevention) as a significant data-related challenge by both line-of-business IT and IT security personnel. DX cannot be complete without robust, dynamically evolving cyber protection. Although cybersecurity and data protection have traditionally been treated as separate disciplines, they are quickly merging into complementary and linked capabilities.

Cyber protection gives Acronis an opportunity to separate itself from the traditional data protection and recovery software vendor pack, by applying a platform of solutions to help customers and partners tackle increasingly complex data protection initiatives and threats. Acronis is well positioned to leverage its investment over the past two years in AI and blockchain technology; its service provider partners and end-user customers will be the beneficiaries.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com