White Paper

Addressing Cybersecurity and Data Protection Holistically with Cyber Protection

Sponsored by: Acronis

Phil Goodwin Frank Dickson

April 2021

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 12 months – and, we believe, tongue in cheek, that the other 7% of 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 further shows that 60% of organizations have completed digital transformation (DX) projects with the intent of being "data driven." DX initiatives are seen as critical projects to improving the competitiveness of the organization by feeding faster, more accurate decision information to business leaders. This research shows that data availability is a key factor in more than half of ITX projects and consumes about one-third of the ITX budget.

IT transformation (ITX) 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. The majority of organizations now have data stored in the core, cloud and edge, often siloed due to different data management tools and policies. According to IDC research, data security is cited by IT professionals and the component of data privacy and compliance that requires the greatest attention in 2021[1]. Among those we surveyed, 32% cited advanced malware as the number one source of breaches[2].

Data availability and security is 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 cyber security – is a key to mitigating risk.

[1] Source: Data Protection and Privacy Survey, IDC, December, 2020. N = 411
[2] Source: EDR and XDR Survey 2020 Survey, IDC, December, 2020. N = 367

IDC recommends that IT organizations take the following actions:

1. Embrace an ITX strategy of cyber protection by more closely integrating data protection, disaster recovery, and cybersecurity operations.
2. Design cyber protection into infrastructure architectures, not as an add-on.
3. Leverage automation and artificial intelligence / machine learning to maximize responses to evolving threats.

SITUATION OVERVIEW

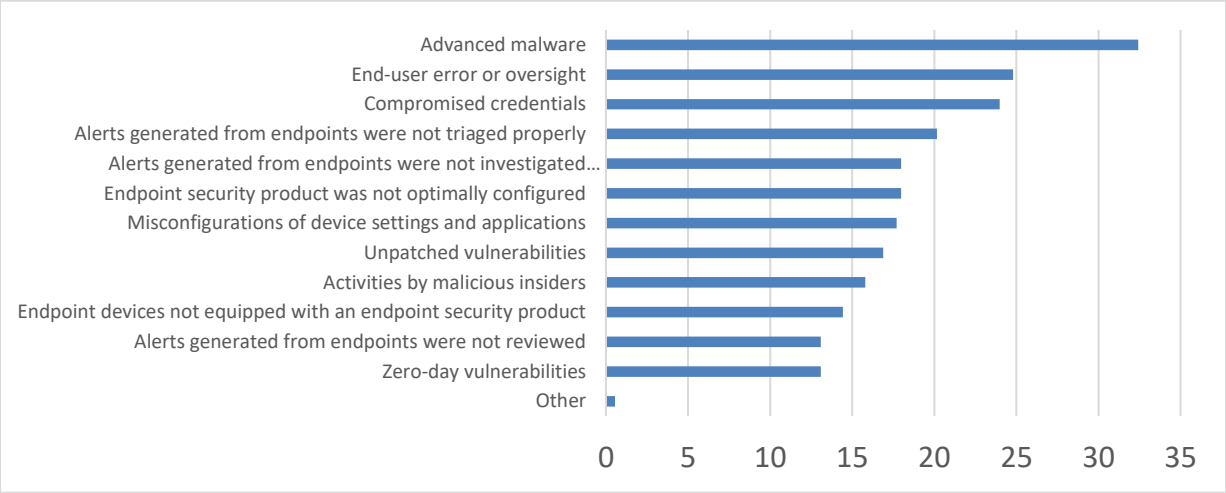
No one is immune to cyberattacks, whether corporation, governmental agency, or individual. Attack sophistication is constantly evolving and improving: it is a veritable arms race between legitimate organizations and cyber criminals. These attacks may be attempts at gaining sensitive information such as personal identities, account credentials, and credit data. In other cases, the target may be corporate or government secrets. As important, 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.

At the same time, the IT environment is becoming more complex while cybercriminals are getting better at identifying and targeting these intrinsic weaknesses. In IDC's recent study of security professionals, complexity is a common theme leading to security breach as 18% cite misconfigurations of device settings and applications, 17% unpatched vulnerabilities, and 25% cite end-user error or oversight as contributing to their most recent breach[3] (Figure 1).

Figure 1

Contributors to Breaches

Q. Which of the following were the most frequent contributors to security breaches?



Source: EDR and XDR Survey 2020 Survey, IDC, December 2020. N = 367

Source: IDC, 2021

[3] EDR and XDR Survey 2020 Survey, IDC, December, 2020. N = 367

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 multi-cloud), 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 a complementary IT discipline. It enlists the skills of traditional backup/recovery, disaster recovery, 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. Increasingly, IT leaders are viewing cybersecurity and cyber protection holistically and are seeking solutions that seamlessly integrate the two to better protect data and simplify implementation and operations.

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 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 anti-virus.

Cyber protection tools may be separate or incorporated with threat detection software. These components include backup, offsite data storage and 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.

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 situations 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, are contributing to the increased importance of scalable means to ensure and publicly attest to data integrity. Companies, their customers, their business partners and other stakeholders (e.g., parties in lawsuits pursuing e-discovery) 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, that what was stored or backed up and what was recalled from storage or backup is identical. Blockchain technology is emerging as exactly this kind of method for ensuring data authenticity.

We believe that AI (for behavioral detection and termination of cyber threats) 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. Operations, line-of-business IT, and IT security practitioners are in agreement that the already-heavy burden of security and compliance 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 technology vendors at the forefront of developing cyber protection solutions that integrate data protection, cybersecurity, and endpoint management capabilities. The Acronis cyber protection platform includes a worldwide network of cloud data centers capable of offering endpoint security and backup as a service (BaaS) for customers and service provider partners as well as on-premises backup and endpoint security. This solution is designed to protect servers, virtual machines, traditional applications, cloud-native applications, edge and mobile devices, remote work and collaboration applications, and any combination thereof. This can include hybrid cloud (on-premises to public cloud) as well as multi-cloud (public to public cloud). This broad architectural coverage helps ensure that an entire environment is under the Acronis cyber protection umbrella and meets data sovereignty requirements. Acronis describes its cyber protection strategy as being focused on five stages of cyber protection, and the company integrates these stages across its product portfolio:

1. **Prevention –** stopping attacks or unintended issues before they happen. For prevention, Acronis provides vulnerability assessments, patch management, zero-day exploit prevention and configuration management tools. The company has also developed a proprietary hard drive health detector that can accurately predict drive failures before they happen. Additionally, Acronis manages a global network of cyber protection operations centers that feeds threats – whether they are manmade or "acts of God" – into an alert system that makes recommendations for customers. For example, if a typhoon is spotted in a customer's region, the system would recommend a comprehensive backup in the event that disaster recovery is required.
2. **Detection –** identifying attacks or unintended issues when they occur. For detection, Acronis has AI-based static pre-execution and behavioral malware and threat detection that is designed to ensure the security of data, applications, and systems by automatically detecting (and terminating) ransomware attacks and other malware incidents. Additionally, Acronis has cloud reputation detections and URL filters to prevent users from inadvertently accessing malicious sites such as phishing pages.
3. **Response –** Acronis's integrated approach simplifies responding to attacks or unintended issues with countermeasures, and in many cases with fully automated responses. For example, Acronis blocks malware from executing through machine learning, as well as removes any downloaded malware. It provides automatic file recovery from backups following ransomware attacks. The company's solution also scans backup files to ensure recoveries are malware free, reducing the chance of reinfection.
4. **Recovery –** restoring clean versions of data and/or applications. For recovery, Acronis draws from its roots in backup and disaster recovery software to provide instant and automated recovery options, ranging from the file level to entire images on similar or dislike hardware or virtual machines. Automated disaster recovery provides instantaneous failover of production systems, while an orchestrated runbook helps prioritize what systems get turned back on, and when. The company's technology can also automatically patch known vulnerabilities before restoring a system.
5. **Forensics –** providing detailed information to help with incident investigations and audits. For forensics, Acronis can provide metadata and memory dumps of workloads together with the backups for detailed incident investigations.

These capabilities are integrated across the entire Acronis portfolio, which is sold directly to enterprise organizations and delivered through the channel by cloud service providers (CSPs) telcos, and hosting providers (i.e., managed service providers [MSP]). This includes foundational technologies and solutions such as:

- **Acronis Cyber Cloud** is a multi-tenant cyber protection solution designed for both private cloud and service provider deployments. This includes automated provisioning, the ability to package, bundle, and price products, and a white-label or co-label option.
- **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 computing and storage infrastructure.
- **Acronis Cyber Platform** is a developer 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.

These cyber protection capabilities are integrated into the following products:

- **Acronis Cyber Protect** integrates full-stack anti-malware protection and endpoint management with advanced backup capabilities for physical and virtual workloads, endpoints, and structured and unstructured data, whether on-premises, in the cloud, or in hybrid clouds. It also integrates patch management, vulnerability assessments, URL filtering, and AI-powered hard drive failure detection.
- **Acronis Cyber Notary** is a blockchain-based service for file notarization, e-signing, and data verification.
- **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** 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.

Service providers can build their services using a single solution that includes the company's essential cyber protection capabilities. Advanced packs can be added to extend the capabilities as needed.

- **Acronis Cyber Protect Cloud** -- installed via one agent and managed through one central console, this product integrates cybersecurity, data protection, and endpoint management in a single solution that protects endpoints, systems, and data. The essential capabilities include full-image and file-level backup and recovery for workloads on more than 20 platforms; an advanced AI-based behavioral detection engine that stops malware, ransomware, and zero-day attacks on client endpoints; and centralized management that integrates with RMM and PSA systems. Vulnerability assessments, file sync and share, blockchain-based notarization, and disaster recovery are also included, incorporated into the following Advanced Pack add-ons:
  - **Advanced Backup** extends the solution's capabilities with continuous data protection, data protection mapping and compliance reporting, scheduled backup reports, and support for Microsoft SQL Clusters, Exchange Clusters, Oracle DB, and SAP HANA.
  - **Advanced Disaster Recovery** enables additional DR features, including production and test failovers, VPN-less deployments, orchestrated runbooks, custom DNS configuration, and IPsec Multisite VPN support / L2 site-to-site open VPN.
  - **Advanced Management** adds automated patch management, software inventory control, disk drive health monitor, fail-safe patching, and report scheduling.
  - **Advanced Security** includes full-stack, next gen anti-malware protection, URL filtering, exploit prevention, malware scanning of data in the Acronis Cloud, forensic data captured in backups, automatic allow listing, remote device wipe, threat feed, and malware reinfection prevention.

By integrating all of the above into a single solution with one agent and managed via one management console, Acronis can deliver several unique capabilities to the market:

- **Continuous data protection**: By defining the list of critical apps for every device that users are working with most often, Acronis' agent monitors every change made in the listed applications. In case of a malware infection, data can be restored from the last point with the latest collected changes so no data is lost. This provides near instant remediation with close to zero RPOs.

- **Safe recovery**: By integrating AV updates and patch management into the recovery process allows the restoration of an operating system image with the latest patches, reducing the change or a recurring infection.

- **Malware scans in the Acronis cloud**: Acronis helps prevent restoring infected files from backups by scanning full disk backups at a centralized location. This can find potential vulnerabilities and malware infections and ensures a malware-free backup.
- **Fail-safe patching**: Since a bad system patch can render a system unusable, Acronis creates an image backup of selected machines before installing a system or application patch, thereby enabling quick rollback of endpoints to a working state if needed.

Acronis has designed its solutions to offer service providers and enterprise 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 malware 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 cyber security into the new discipline of cyber protection will play an important role in the success of DX initiatives. The 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. It represents a new problem set for which a majority of backup/recovery vendors do not yet have a solution. Acronis is well positioned to leverage its investment over the past several 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

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com