White Paper

Five Key Technologies for Enabling a Cyber-Resilience Framework

Sponsored by: IBM

Phil Goodwin Sean Pike

June 2018

IDC OPINION

IDC's recent security surveys show that 50% of security professionals now spend most of their time securing the cloud and that over the prior 12–18 months, many experienced what they described as a cloud-related breach. Some 23% of respondents indicated that they had fallen victim to a ransomware attack, 22% said they had experienced an IoT breach, and 23% reported that they had experienced a DDoS attack. About 75% of those attacks occurred because of some cloud-related incident.

This isn't to say that cloud-related technologies and new ways of communicating are the *root* cause of breaches and business failures; rather, it's to say that as businesses adopt new technologies, their protection strategies must change to keep pace. These strategies must include stronger and more varied security mechanisms, but they must also include ways to recover quickly should a breach or an incident occur.

All over the world, enterprises are steadily making their way through digital transformation — the process of integrating technology with all aspects of the business to accelerate business activities, support agility, and capitalize on strategic vision and dynamic opportunities. A key element of digital transformation is becoming a data-centric organization capable of monetizing information. At the same time, digital transformation inherently brings with it new risks that may have been previously unforeseen or that may have complicated the risk profile of well-established business processes. As a result, enterprises seek higher levels of integration between key business support functions and greater data availability to ensure that the business is ready to withstand any challenge. This is cyber-resilience.

Cyber-resilience combines the best practices from IT security, business continuity, and other disciplines to create a business strategy more in line with the needs and goals of today's digital business. In this IDC white paper, we describe how digital transformation is breaking down the traditional safeguards between enterprises and participants in the global economy as business-enabling technologies become gateways to risk, attack, and failure. This white paper further describes how cyber-resilience practices can help enterprises defend against those risks and recover from breach or failure in a controlled, measurable way. Finally, it provides a framework to help organizations begin to engage in their cyber-resilience journey and provides strategies to modify data protection and recovery practices to better align with today's more targeted and malicious attacks.

IN THIS WHITE PAPER

Is today the day that your business operations come to a screeching halt? Is today the day your business is shuttered? It's a pessimistic view of the reality of business. At any moment, some event that upsets the operational fabric of the business could occur, and in today's fast-paced business world, every second counts.

Events don't have to be catastrophic to have a lasting impact. Most mature businesses already practice risk management and some measure of business continuity or resilience. Those organizations likely have an understanding that large events with devastating impact have a lower likelihood of occurrence than do small, discrete events that might cause an operational ripple. Take for instance the avian flu scare: Many may remember a time in the mid-2000s when businesses were hyperfocused on the potential impact a rapidly moving airborne virus might have on employees and business operations. While the concept is certainly something worthy of concern, the likelihood of the avian flu or similar threat materializing was and remains very low. That low likelihood didn't stop organizations from trying to create operational contingencies based on the nature of potential impact. The same is true for other natural disasters or physical threats. The potential for high-stakes outcomes drives consideration, and sometimes, focusing on the potential scale of a single event can distract organizations from focusing on the very real, tangible, and discrete threats that can have a devastating business impact.

Digital transformation is challenging traditional views of business resilience. Digital transformation is the process through which technology is intertwined throughout the human experience. In the enterprise, digital transformation means a higher level of connectivity between applications and business processes with the aim of increasing business agility and connecting more readily with customers and business partners with the expectation that users have 24 x 7 uninterrupted experience. Digital transformation can come in many forms. A business may be seeking to better integrate existing infrastructure and legacy systems or slowly wading into the cloud, or it may have a cloud-first mandate. Regardless, the concept of a connected enterprise becomes critical when assessing business resilience. Whether this involves tying together business processes or developing hybrid cloud or multicloud environments, as business systems and processes become hyperconnected, there is a greater likelihood that a discrete event could upset the entire business. What was once a small ripple could now send shockwaves throughout the entire organization.

It's for this reason that cyber-resilience has become of paramount concern for security professionals as well as for those responsible for business continuity and risk management planning. Cyber-resilience is the merging of cybersecurity, risk management, and business continuity/resilience practices to create a discipline focused on improving cyber-response capabilities from event detection and recovery to continual process improvement. Clients are recognizing that traditional business continuity strategies focused on system failures and outages need to evolve and focus on cyber-based threats that maliciously target your data. The traditional recovery procedures for a system outage will most likely not protect you from a cyberthreat corrupting your data.

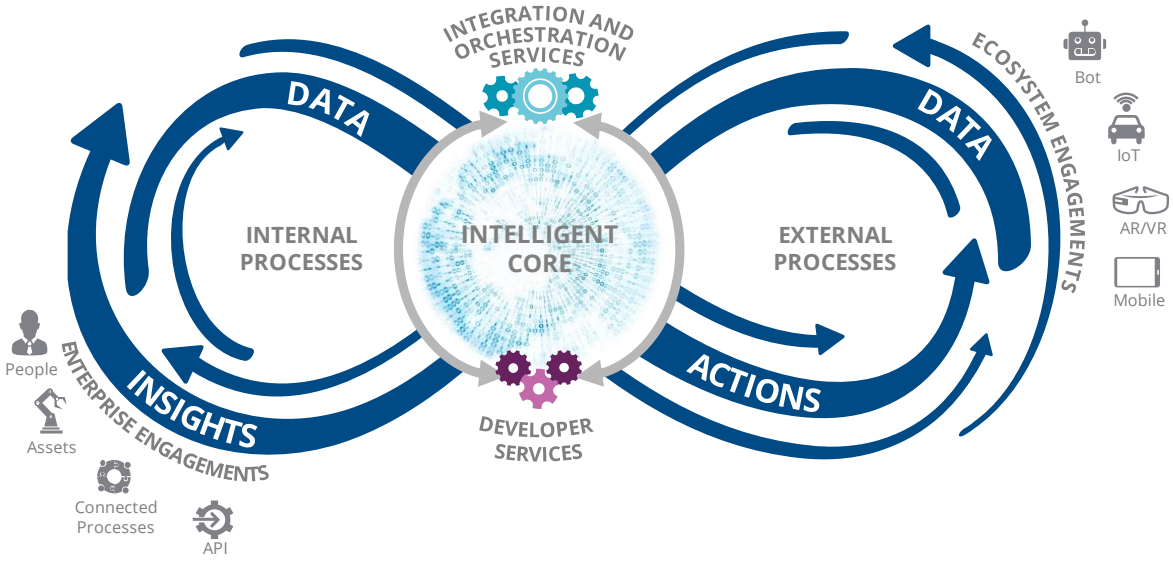
The Rise and Flaws of Digital Transformation

In 2017, businesses spent $1.1 trillion trying to transform into connected, intelligent, and technology-driven organizations. In 2018, businesses will spend an additional $1.3 trillion. By 2021, businesses worldwide will be spending as much as $2.1 trillion per year just trying to transform, and that number figures to only continue increasing. IDC believes that by 2020, only about 60% of organizations will have embarked on a digital transformation journey and 70% of CIOs will have developed a cloud-first strategy to support the infrastructure agility required by transformation. That leaves a tremendous amount of digital transformation growth opportunity as much as three years from today.

Why so much spending? Simply put, businesses believe that digital transformation is the path forward in a hyperconnected world. Companies must find innovation and agility to survive, and they must be prepared to go to market rapidly, at scale, with new products and services while developing the key insights necessary to reach core audiences and open new markets. In fact, IDC believes that the height of transformation for most organizations will see them leverage an intelligent core infrastructure that turns business activity insight into actionable intelligence in a streamlined, continuous process. IDC describes this as the digital transformation platform (see Figure 1). At its center, this platform relies on diverse, distributed, and dynamic data to drive opportunity.

FIGURE 1

Digital Transformation Platform: A Framework for the Intelligent Core



Source: IDC, 2018

Without data the model fails. Data can no longer be productized and monetized. Data can no longer be leveraged for business agility. This makes data critical to business survival and, in turn, makes data integrity and accessibility sacrosanct. However, the attributes and location of data relevant to a digital transformation platform continue to change. Data has become increasingly diverse, spanning not only structured systems but also unstructured data such as time series data, machine-generated data, and stream data. Data is also increasingly more dynamic; it not only is based on batch runs but also is real time in nature as telemetry data is generated from a growing number of sensors and devices.

In addition, data is increasingly distributed, located not only in core datacenters but also in edge locations, on devices, and in cloud services. Data being diverse, dynamic, and distributed further exacerbates the ability to employ an effective cyber-resilience program.

This isn't to say that data is the only consideration. For most organizations, their journey into digital transformation starts with a series of loosely connected systems that they hope can be established as an interconnected system. Let us think about digital transformation in terms of a Rube Goldberg machine. For the uninitiated, Rube Goldberg was an engineer, an inventor, and a Pulitzer Prize–winning cartoonist who ultimately gained widespread fame for drawings of complex systems in which he would depict common household items being strung together working to complete some mundane task. If this sounds familiar, it should. Businesses are stringing together HR systems, contract management, ERP systems, customer-facing applications, and more in the hopes that they will operate in a common, business-forward direction. This is where digital transformation starts to demonstrate a challenge for those charged with reducing a business' risk.

What happens when you place a broom handle in the spokes on a bicycle wheel? If the spokes aren't connected to anything, then probably nothing will happen; however, the spokes on a wheel are connected. When one or two spokes are impeded by a foreign object, the whole wheel stops turning. That is the risk of interconnected business systems. When a single system fails, it could mean the business ceases to function.

In terms of cyber-resilience, this means any single business process could represent a gateway to other business processes. It means the attack surface of one process has the potential to grant lateral access to nearly any other process.

Challenges in the Digital Transformation Journey

While the spending on digital transformation is impressive, IDC already sees increasing external pressures beginning to have a significant impact on the cybersecurity strategy of organizations. As mentioned previously, the interconnection of systems and the continued reliance on external services such as cloud and IoT will bring risks that many organizations are not prepared for today.

IDC estimates that by 2020, about 60% of organizations will have embarked on a digital transformation journey and 70% of CIOs will have developed a cloud-first strategy. While that number is impressive, it is not clear how many of these organizations recognize that data and application (information) availability is core to digital transformation success. Without availability, data cannot be monetized. Greater information availability will give companies a relative competitive advantage over companies that struggle with availability. Even though IDC has seen increased spending around anti-DDoS products and services, many customers struggle to put forward a coherent strategy for information availability that provides rapid, end-to-end preservation of data/information availability through the entire process of data access.

Another external challenge for organizations is the rise of regulatory compliance. By 2025, more than 70% of corporate data will fall under regulatory compliance. This data not only requires special handling but also creates additional risks to the organization, which could suffer harsh penalties for improperly protecting data.

Increasing Reliance on Cloud and IoT

Data availability and compliance are both external forces that significantly impact the business, but at the same time, they may only be indirectly affected by the business. This is especially true as more businesses rely on cloud and IoT devices for business-critical functions.

Organizations today are using hybrid cloud, and most future applications will be cloud enabled. In a recent survey, organizations reported that half of their workloads are deployed in a hybrid cloud model today. This same cohort plans to have 62% of their workloads running in hybrid cloud within the next two years. Security is both a driver and an inhibitor for hybrid cloud adoption. Critical data is now spread across numerous geographies, datacenters, and cloud. This data must be protected according to corporate requirements, regardless of where it resides. Organizations surveyed are expecting a 40% increase in spend on data services for hybrid cloud over the next 12 months. Backup and recovery and data costing/value assessment are the top priorities.

Companies are increasingly gathering more and more sensitive data not only from the cloud but also from IoT devices. While these devices often have lower processing power than full systems, attackers have illustrated capabilities in leveraging IoT devices as part of their attack strategy. That capability, combined with a general lack of security around IoT devices, means organizations must determine how to best defend IoT devices that may be difficult to access, monitor, and secure, in addition to traditional computing devices.

Increasingly Complex Outages

While IDC has seen organizations display more confidence in their ability to secure the cloud and the rate of movement to the cloud and adoption of cloud-based security solutions has been increasing, one challenge that organizations appear less prepared for than ever is the increasing complexity of outages.

In a recent IDC customer survey, 56% of respondents indicated that they had experienced a DDoS attack that lasted 5–24 hours. Another 8% of respondents said that they had experienced an attack that lasted 1–7 days, and even more alarming is that 6% of respondents indicated that they had experienced an attack that lasted 8+ days.

Backup and disaster recovery (DR) are insufficient protections against modern threats. IDC best practice recommends a one-hour RTO for mission-critical apps and a four-hour RTO for noncritical apps. Certain point-in-time (snapshot) copies can be incomplete, inefficient, and vulnerable to attack when designed improperly. Often the approach is designed for system-level recovery and not environmental recovery such as platform or configuration corruption. Poor maintenance and testing hygiene can also sabotage robust point-in-time data copy protection schemes.

IDC research reports that the "average" cost of downtime exceeds $200,000 per hour, although this varies by company size and industry. Generally, these costs can be used to help guide organizations when making determinations in building remediation plans and infrastructure. Cost estimates include actual loss of revenue and costs for recovery, including regulatory costs, which may be severe. These estimates do not include reputational cost and long-term brand damage that might occur from an embarrassing breach. These cost estimates, however, can be used to help determine the appropriate organizational spend on breach remediation infrastructure strategy. A recent ransomware example is illustrative. The city of Atlanta recently spent nearly $3 million on emergency efforts in the three weeks following a ransomware incident that disabled certain city services. The city has reportedly asked for an additional $9.5 million to recover and strengthen defenses. While an additional $9.5 million in resources may sound extreme, if you anticipate avoiding additional $3 million ransomware expenditures for the foreseeable future, the $9.5 million one-time bolstering of defenses seems much more reasonable.

Advanced Attacks on the Rise

IDC also continues to see a rise in the number of advanced attacks. Industry statistics show that many attacks stay undetected for well over 200 days. With so much time to hide in a network, attackers can plant malware that finds its way into the backup sets; as a result, the recovery data is also infected. Attacks may stay dormant for weeks or months, allowing malware to propagate throughout the system. Even after an attack is detected, it can be extremely difficult to remove malware that is so prevalent throughout an organization.

SITUATION OVERVIEW

The Cyber-Resilience Concept

Infrastructure resources are increasingly available in the cloud and across IoT devices. However, traditional defenses to successfully counter the emerging threats are proving ineffective. As a result, organizations must take a new approach to security. Today's threat landscape demands an integrated solution that spans the data life cycle. Organizations must focus on shortening the life-cycle stages between defense and detection and response and recovery to build a cyber-resilience capability.

The Cyber-Resilience Framework

Cyber-resilience is a framework designed to help organizations withstand attacks. It is not a single layer of protection or a single product but a way for organizations to structure their defenses such that no one event is catastrophic. Cyber-resilience is an iterative process that provides the means of recovery from an attack. Compared with traditional defenses that were useless once bypassed, cyber-resilience allows a constant vigilance across the organization.

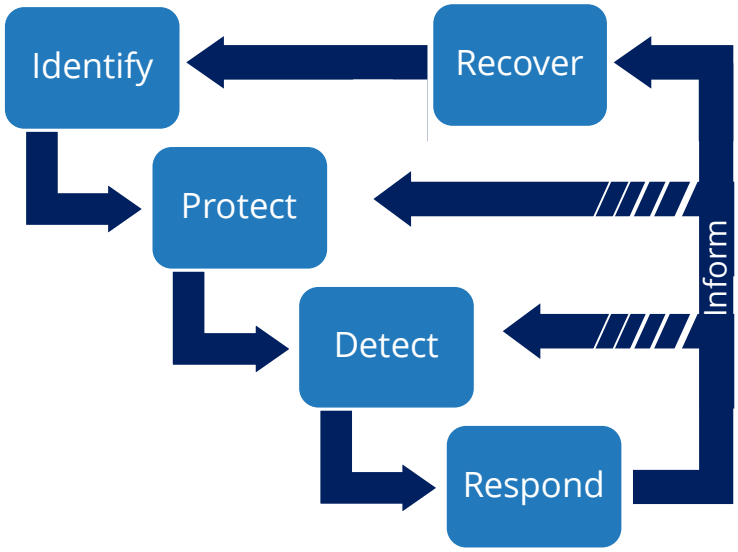
The five components of the cyber-resilience framework are (see Figure 2):

- **Identify:** Critical asset and process mapping, risk and readiness assessment, and so forth
- **Protect:** Traditional first line of defense security mechanisms
- **Detect:** Security analytics
- **Respond:** Response to security breaches or failure
- **Recover:** Coordinated recovery mechanisms

The key advantage of the cyber-resilience framework is that it puts business forward. Traditionally, security has operated as an overlay to the business. Cyber-resilience integrates security into the business itself, allowing for the five components to be present in all areas of the business.

FIGURE 2

Cyber-Resilience Framework



Source: IDC, 2018

The Event Versus the Aftermath

Time and time again the industry has shown that attacks will be successful. Security is complex, and there is simply no way to prove that an environment is secure. Attackers continue to use innovative methods to get into organizations, resorting to whatever tactics are necessary to launch a successful attack. The best an organization can hope for is a hardened infrastructure, auditable functions and processes, well-trained users, a crack security staff, and continuous monitoring processes. That would be a great position to be in. The key for most organizations, however, may be to create a renewed focus on what happens after an attack. If, with a laundry list of controls and checks and balances, we already know an attack will be successful at some point, doesn't it make sense to prepare for the aftermath? When an attack is successful, businesses must find a way to shorten the cycle between detection and response and the cycle between response and recovery. The closer a business can get to achieving continuous operations, even in the wake of a successful cyberattack, the better.

The business entity is unforgiving. It does not care how advanced an attack is or how the attacker succeeded in infiltrating the organization. The business must persist. By taking advantage of strategies to lower operating times in detection, response, and recovery, organizations not only can lower the cost of an incident but also ultimately can create a competitive advantage. IDC believes that businesses that can minimize disruptions will have a significant advantage over ill-prepared businesses in creating trust with consumers and business partners.

FUTURE OUTLOOK

Five Key Technologies of Cyber-Resilience

While the cyber-resilience framework might seem intuitive on the surface, it must be implemented through careful selection of technologies. There is no one product that can create a cyber-resilient environment, but there are key technologies that an organization can implement to address the potential of business disruption from a cyberattack. The five technologies described in the sections that follow are instrumental in allowing organizations to create a resilient environment.

Automation and Orchestration for Recovery of Platforms and Application Data

Automation has long been a scary term for security professionals. Concerns around automatic response have been widespread throughout the industry for as long as automated solutions have existed. However, in today's widely automated attack environment, intelligence automation is key. Instead of relying on automation as the solution, orchestration and automation must become part of the response.

Orchestration is not about taking humans out of the equation or allowing blind policy changes, but it is about augmenting analysts, giving them rapid access to information and the ability to respond faster than they could manually. Further, successful recovery of applications requires a multistaged recovery of interconnected systems and data. The manual recovery of these systems can introduce human error, while codification of recovery processes through software templates that are validated and tested can mitigate risk in the recovery process.

Air-Gapped Protection as a Fail-Safe Copy Against Propagated Malware

Air-gapping refers to physically or virtually separating systems or networks from other systems or networks. Companies, for instance, may choose to completely separate networks or systems that contain highly sensitive data from the day-to-day operational network.

While the perimeter has disappeared and businesses expect fluidity in their data across the organization, the ability to create air-gapped segments of the network is more important than ever before. As we have seen with recent infections of ransomware, an automated piece of malware can be designed to quickly traverse the network, quickly creating havoc. This leaves an organization exposed internally and potentially externally depending on the system or systems impacted. Today, best practice is to create an air-gapped copy of critical data to mitigate external exposure, protect the organization from operational downtime, and avoid unnecessary costs.

Write Once, Read Many/Immutable Storage Technology to Prevent Corruption or Deletion

The recent success of ransomware attacks such as NotPetya has illustrated the need for stronger protection against the corruption or deletion of data. It is well known that attackers look to erase logs in order to cover their tracks, but the deletion or corruption of data can destroy a business. In the wake of WannaCry and other recent ransomware attacks, many organizations found that even paying the ransom did not result in attackers turning over the encryption key. In some cases, the key provided by an attacker did not work at all.

Organizations need to have technologies in place that provide unalterable data. Write once, ready many (WORM)/immutable storage technologies can address this need. Using WORM/immutable storage technologies, an organization can maintain the integrity of its data and maintain business resiliency against what have been some of the most crippling attacks seen in recent times. Multiple forms of WORM technology exist at the software layer and the hardware layer. Both offer a means to ensure data is not tampered with and to provide an electronic chain of custody.

Efficient Point-in-Time Copies and Data Verification to Quickly Identify Recoverable Data

Once an attack has occurred, organizations need a way to validate and rapidly recover a good copy of data. As mentioned previously, many attackers are living inside of networks for close to a year, meaning that often backups are also infected. This is the reason a highly efficient point-in-time technology is needed to maintain multiple copies of data. Continuous data verification is necessary on these copies to proactively identify potential infections and take corrective actions. It also helps quickly identify good data copy for the recovery process. There are different approaches to backup data verification, with features incorporated into both hardware and software to ensure data has not been infected.

Data verification is mandatory with disaster and operational recovery testing processes. First, you want to ensure the backup/replicated data has integrity and the backup/replication performed as expected. Second, you want to inspect the backup/replicated data to ensure the same infection that occurred in the production data was not also spread to the backup/replicated data. Depending on the system that is being backed up, users may want to employ multiple different data verification techniques. For example, a database system may have native triage and inspection tools that are useful to complement capabilities within a broader data protection solution.

Regulatory Reporting and Assurances

While regulatory compliance often gets a bad reputation for being a checkbox that does not improve the overall security of an organization, the truth is that validating that proper controls are in place and effectively operating on data can be extremely effective. In addition, with growing fines for noncompliance, having effective reporting can help organizations prove they are complying with regulations and save both time and money associated with costly audits and potential penalties.

CHALLENGES/OPPORTUNITIES

Cybersecurity is the leading challenge in today's business climate. The pace and volume of security threats are challenges for organizations of any size to keep ahead of. This places even more importance on the planning for and deployment of cyber-resilience strategies. An effective cyber-resilience strategy is broad in scope and stakeholders, bringing together different constituents. Key stakeholders include not only security, operations, engineering, legal, and risk professionals but also data owners and line-of-business executives. This requires collaboration and planning across organizations with different priorities and depth of knowledge. This organizational dynamic is a challenge commonly seen in larger organizations, but it can be addressed through C-level strategic planning and priority setting.

CONCLUSION

Cyber-resilience is key to data and application availability. It is also a key component of the digital transformation journey. Without proper cyber-resilience, organizations will find themselves more and more susceptible to attacks that can paralyze a business. In addition to malicious attacks, the increasing number of regulations spanning different geographies and industries can render a business at risk of serious fines without continuous validation of controls.

The practice is also more than mere malware detection, backup, or DR. It is an integrated life-cycle approach to providing data availability against all threats, including the platform. Cyber-resilience must span both on-premises and cloud repositories. IT organizations must take a comprehensive approach to cyber-resilience and look for products that address the breadth of cyberthreats.

Finally, cyber-resilience is a framework for recovering from attacks. However, a solid collection of underpinning technologies is required to ensure that each step of the framework can be addressed. Security can no longer be described in terms of varying levels of confidentiality, integrity, and accessibility; it must encompass all three pillars at all times. Organizations that implement cyber-resilience will find themselves at a competitive advantage in the future as customers will find gaps in the availability of businesses. A resilient organization is an organization that can adapt and recover from attacks.

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