



THRIVING ON THE EDGE OF CHAOS

A Holistic Approach to Organizational
Cyber Resilience



Contents

Introduction	1
Background	2
What is Digital Value?	3
What is Digital Risk?	5
A New Paradigm	7
Organizational Leadership	10
Organizational Assessments	12
Connecting Digital Business Outcomes to Culture	13
Final Thoughts	15

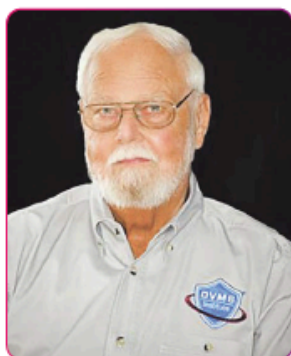
Introduction

Protecting Organizational Digital Business Performance, Resilience, and Trust.

The Institute's Mission is to teach organizations of any size, scale, or complexity how to protect the value and resiliency of their digital business ecosystem

The Institute's Vision is to teach organizations how to leverage the NIST Cybersecurity Framework and the Institute's Digital Value Management Overlay System to manage organizational cyber risk and resilience

As Cloud Services revolutionized the creation and management of digital infrastructure, the DVMS NIST Cybersecurity Framework Overlay System™ will revolutionize how organizations operationalize a culture capable of mitigating cybersecurity risk that meets the stringent cybersecurity expectations of government regulators and business stakeholders.



David Nichols
Executive Director



Rick Lemieux
Executive Director
of Programs



David Moskowitz
Executive Director and
Content Architect



Lori Perrault
Director of Operations

Background

The digital landscape has fundamentally changed how businesses operate, compete, and engage with customers in today's digital marketplace. This shift has brought new risks and challenges that call for a proactive and strategic approach to protecting the value delivered by digital assets.

Digital assets, including data, intellectual property, customer information, and technological capabilities, are vital to today's digital enterprises. Protecting the value delivered by those assets is not just a matter of compliance but a strategic necessity to ensure that digital business quality and reliability objectives are met.

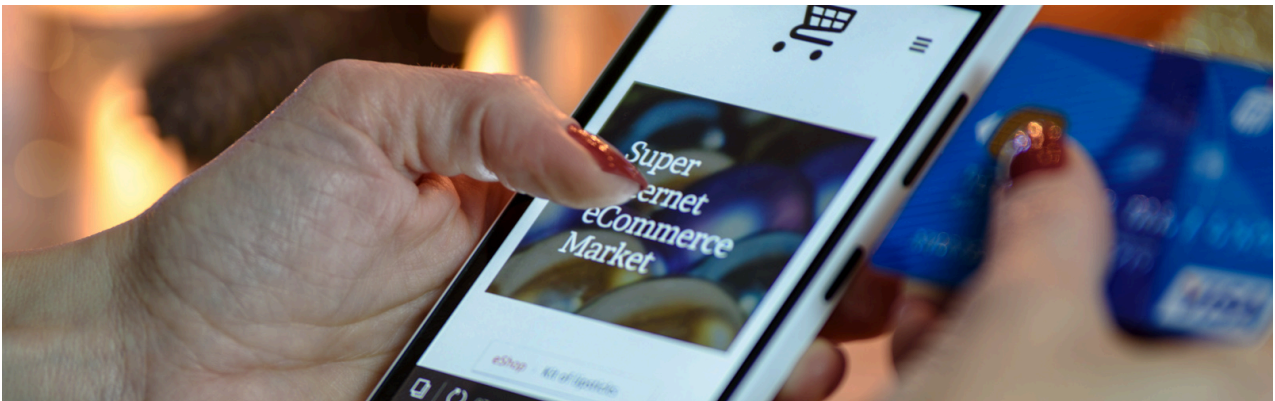
Governments, CEOs, and boards must acknowledge the importance of safeguarding the quality and reliability of digital assets to ensure long-term sustainability and success. Organizations prioritizing protection can gain the trust of their constituents, clients, and investors by demonstrating their commitment to safeguarding the digital assets that underpin critical infrastructures and the global economy.

Conversely, neglecting investment in protection can lead to severe consequences, such as disruption to digital business operations, ransom demands, fines, lawsuits, regulatory sanctions, remediation costs, customer satisfaction issues, and potentially human lives.

What is Digital Value?

The digital landscape has changed significantly over the past few decades, fundamentally altering how governments and businesses create value. From the early days of the internet to the rise of mobile computing and the advent of artificial intelligence, digital technologies have revolutionized industries, disrupted traditional business models, and created new growth opportunities.

The emergence of e-commerce marked a significant milestone in the evolution of digital business value. Online retailers like Amazon and eBay demonstrated the power of digital platforms to reach a global audience and facilitate previously impossible or impractical transactions. The success of these early e-commerce pioneers paved the way for other industries to adopt digital channels and explore new business opportunities.



The rise of mobile computing transformed the way businesses create and capture value. Smartphones and tablets have become ubiquitous, providing consumers with unprecedented access to information and services. Businesses that have been able to adapt to the mobile-first era have seen significant benefits, including increased customer engagement, improved sales, and brand loyalty.

Artificial intelligence (AI) has emerged as a powerful force in the digital landscape in recent years. AI-powered technologies, such as machine learning and natural language processing, automate tasks, improve decision-making, and create personalized customer experiences. Businesses that can harness the power of AI are gaining a competitive advantage and unlocking new sources of value.

Data has also become an asset for businesses, enabling them to gain insights into customer behavior, optimize operations, and develop new products and services. Companies that can effectively collect, manage, and analyze data are better positioned to create value in the digital age.

As the digital landscape evolves, governments and businesses must adapt to protect national security and stay competitive. This requires a focus on innovation, a willingness to embrace new technologies, and a commitment to delivering value to customers. By understanding the trends shaping the evolution of digital business value, organizations can position themselves for success in the digital age.

“The digital landscape demands continual learning and adaptation at the individual level, which contributes to, and is crucial for, team success. This mental model stresses the importance of embracing change, experimentation, and innovation to stay competitive and deliver sustainable digital value, with the understanding that the perception of value changes over time.”

Thriving on the Edge of Chaos – Moskowitz & Nichols

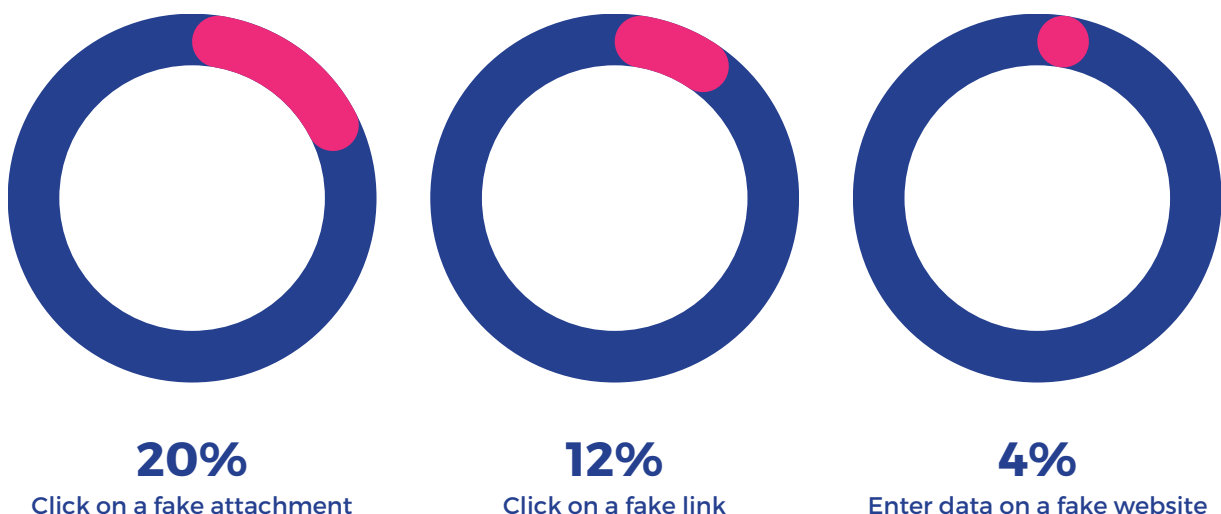
What is Digital Risk?

The digital age has brought unprecedented advancements, transforming how we live, work, and interact. However, with these advancements come inherent risks that threaten our privacy, security, and well-being. Recognizing and understanding these digital risks is crucial for protecting ourselves and mitigating potential harm.

One of the most pressing digital risks is cybersecurity. As our reliance on technology grows, so does the potential for cyberattacks. Malicious actors constantly seek vulnerabilities in systems, networks, software, and people to steal sensitive data, disrupt operations, or extort organizations. This can lead to financial losses, reputational damage, and operational disruptions.

Another significant digital risk is data privacy. The vast amount of personal data collected and shared online creates opportunities for misuse and exploitation. Data breaches, identity theft, and unauthorized access to sensitive information can severely affect individuals and businesses. Protecting personal data requires robust security measures and responsible data handling practices.

Employee Actions Leading to the Success of Phishing Attacks:



Source: NIRA

Social engineering is a standard digital risk that exploits human behavior to gain unauthorized access or information. Phishing scams, impersonation attacks, and other social engineering tactics can trick individuals into divulging sensitive details or clicking on malicious links. Awareness and education are essential to prevent falling victim to these attacks.

The increasing interconnectedness of digital systems also introduces new risks. Supply chain attacks, where malicious actors target third-party vendors or suppliers, can compromise the security of entire organizations. Additionally, the reliance on cloud-based services can expose sensitive data to potential vulnerabilities if not properly secured.

Digital risks also extend to social media and online platforms. Misinformation, disinformation, and hate speech can spread rapidly, harming individuals, communities, and society. Online harassment, cyberbullying, and the exploitation of vulnerable individuals are other pressing concerns.

To ensure continued success in the digital domain, organizations must understand the shifting landscape of digital risks and take proactive measures to protect digital assets.

A New Paradigm for Protecting Organizational Digital Value

Traditional approaches to protecting digital value have focused on preventing breaches and minimizing damage. However, these approaches are no longer sufficient to address the complex and evolving threats organizations face today. A new paradigm is needed to guide digital value protection efforts to ensure organizations can effectively protect the quality and reliability of their digital assets to provide sustainable value.

At the core of this new paradigm is recognizing that digital value protection is not just a cost center but a strategic imperative. Investments in digital value protection should be viewed as investments in the organizational ability to protect the quality and reliability of its digital assets. This shift in perspective requires a more holistic approach to digital asset protection, considering the immediate costs of digital breaches and the long-term consequences for organizational reputation, operations, and financial performance.

One key element of the new digital value protection paradigm is a focus on resilience. Resilience is the ability of an organization to adapt to changing circumstances and bounce back from setbacks. In the digital context, resilience means recovering quickly and effectively from a breach, minimizing the disruption to business operations, and protecting the organizational reputation. To build resilience, organizations must invest in proactive digital protection measures, develop robust incident response plans, and foster a culture capable of mitigating digital risk to protect digital business data, performance, resilience, and client privacy and trust.

In recent years, there has been a significant surge in cyber threats, highlighting the importance of adequate digital value protection. As organizations grapple with increasingly sophisticated attacks, global regulators have implemented stringent standards to protect sensitive data and mitigate potential risks.

Several pivotal regulatory developments reshaped the digital protection landscape in 2023 and 2024. Among the most significant was the European Union's Digital Operational Resilience Act (DORA), which came into force in 2023 and will become effective in 2025. This legislation imposed stringent requirements on financial institutions, compelling them to bolster their digital business resilience. DORA mandates a risk-based approach to operational resilience, necessitating measures to identify and manage cyber threats, test resilience, and report incidents.

The Securities and Exchange Commission (SEC) finalized its cyber breach disclosure rules in the United States. These rules require public companies to disclose material cyber incidents and their impact on the business. The SEC's mandate aims to provide investors with greater transparency regarding organizational digital value protection practices and vulnerabilities.

Other regions have witnessed regulatory advancements beyond Europe and the United States. Countries like Singapore and Japan have introduced digital protection frameworks and standards to protect critical infrastructure and sensitive data in Asia. These frameworks often emphasize the importance of risk assessment, incident response planning, and digital governance.

One of the overarching trends in recent regulatory developments has been a focus on accountability and transparency. Regulators increasingly demand that organizations take responsibility for their digital protection practices and promptly disclose incidents. This emphasis on accountability is intended to deter cybercrime and encourage organizations to invest in robust digital protection measures.

Another critical aspect of the new digital value paradigm is a focus on data privacy and protection. The new paradigm requires organizations to adopt a data-centric approach to digital information protection, prioritizing protecting sensitive data and compliance with relevant regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

In addition to regulatory mandates, industry standards and frameworks have played a crucial role in shaping digital value protection practices. For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework provides voluntary guidelines for protecting digital businesses. Organizations across various industries widely adopt the framework, which offers a structured approach to identifying and mitigating digital risks.

As the threat landscape evolves, regulatory standards for digital value protection will likely become even more stringent. Organizations must stay informed about the latest regulatory developments and adapt their practices accordingly. By investing in robust digital protection measures and complying with relevant regulations, organizations can protect their sensitive data, mitigate risks, and build trust with their stakeholders.

Furthermore, the new digital value protection paradigm emphasizes the importance of risk-based decision-making. Organizations should assess the risks of different digital threats and allocate resources accordingly. This requires a sophisticated understanding of the organizational risk profile.



Organizational Leadership: The Architects of Digital Value Protection

Beyond safeguarding data, organizational leadership is instrumental in shaping a new paradigm for protecting digital assets. These leaders foster a deep understanding of the digital ecosystem, creating a holistic approach encompassing infrastructure, applications, and user behavior. This proactive stance enables them to identify vulnerabilities, assess risks, and implement effective measures to safeguard digital value.

One defining characteristic of organizational leadership is its ability to anticipate emerging threats. Recognizing the dynamic nature of the cyber landscape, these leaders stay abreast of evolving trends and technologies to address potential risks proactively. This foresight allows them to stay ahead of the curve and mitigate threats before they materialize.

Moreover, organizational leadership must consider the broader implications of digital value protection. By safeguarding data, these leaders contribute to organizational resilience, business performance, and client trust, all essential for growth and innovation.

In addition to technical expertise, effective organizational leadership involves clear communication of complex security concepts to both technical and non-technical audiences. This fosters trust and collaboration with business leadership and stakeholders. Furthermore, these leaders champion a culture of digital value protection, emphasizing shared responsibility and accountability.

Addressing the increasing complexity of the digital landscape poses a significant challenge for organizational leadership. As organizations adopt new technologies and business models, the attack surface expands, making it imperative to stay current on threats and adapt strategies accordingly. Another hurdle is the shortage of skilled digital protection professionals. To address this, organizational leadership must invest in training and development programs to build the skills of their team members and create a supportive work environment that attracts and retains top talent.

Organizational leadership is pivotal in today's digital age. By combining technical expertise, strategic thinking, and effective communication, these leaders protect organizations' valuable digital assets and ensure their quality and resilience in the face of evolving cyber threats.

“Organizational leadership is responsible for its culture because it establishes the norms regarding how and why people behave. The difficulty is: How do you measure it? How do you examine the organization globally? An organization that treats its cyberculture as an unknown will fail as a cyber-resilient organization.”

A Practitioner's Guide to Adapting the NIST Cybersecurity Framework – Moskowitz & Nichols

Organizational Assessments: Identifying and Classifying Digital Risks

A company's cybersecurity strategy depends on its culture, capabilities, and skills. Even with advanced technical controls, these foundational elements are crucial for effective digital risk management. Conducting comprehensive assessments in these areas is essential to identifying vulnerabilities, prioritizing improvements, and mitigating cyber risks.

An organizational cybersecurity culture reflects employees' attitudes and behaviors toward protecting digital assets. To strengthen the overall digital value protection posture, organizations can identify areas requiring additional training by assessing the organizational culture through surveys, interviews, and observations.

Digital value protection capabilities involve the technical infrastructure, processes, and procedures to safeguard digital assets. This includes adopting the NIST Cybersecurity Framework and creating robust incident response plans as a foundation. Evaluating these capabilities entails assessing the effectiveness of current controls and identifying any protection gaps.

Understanding an organization's strengths and weaknesses in digital asset protection can help prioritize investments in areas that need improvement. Individual employees' knowledge, abilities, and experience in protecting digital assets are critical to an organization's overall defense. Assessing digital protection skills involves evaluating the qualifications and experience of all employees, as they all play a role in safeguarding the organizational digital assets. Skills assessments, certifications, and performance reviews can help identify skill gaps.

By investing in training and development, organizations can ensure their team has the necessary expertise to protect the quality and resilience of a company's digital assets.

A Holistic Approach to Connecting Digital Business Outcomes to Culture

Technology often takes center stage as the bulwark against cyber threats in the intricate tapestry of organizational resilience. Firewalls, encryption, and intrusion detection systems are visible armor, their strength meticulously calculated and deployed. Yet, beneath this technological facade lies a less tangible, equally critical component: organizational culture. This cultural undercurrent of shared values, beliefs, and behaviors can fortify or undermine an organizational ability to protect its digital value.

Culture is an organizational DNA, shaping its identity and influencing every action. It's more than just compliance with regulations or policy adherence; it's a mindset permeating every level of the organization. A culture where digital value protection is ingrained in the fabric of daily operations, where employees see themselves as custodians of digital value protection rather than passive recipients of cybersecurity directives.

At its core, culture fosters a sense of shared responsibility. Employees understand that their actions can impact organizational digital value regardless of their role. From the executive suite to the mailroom, individuals are empowered and encouraged to report suspicious activities, question anomalies, and seek clarification when unsure. This proactivity is a potent weapon against cyber threats, enabling early detection and response. Moreover, culture influences employee behavior, a critical factor in digital value protection.

A culture prioritizing efficiency over digital value protection can lead to shortcuts and workarounds compromising data integrity.

Conversely, a culture that values digital value protection as much as productivity encourages employees to follow protocols without compromising their workflow. This balance is essential for long-term success.

Trust is another cornerstone of a robust digital value protection culture. Employees must trust that the organization is committed to their safety and well-being. This trust is built through open communication, transparency, and accountability. When employees feel valued and heard, they are more likely to be engaged in digital value protection initiatives.

Leadership plays an indispensable role in shaping organizational culture. Senior executives' genuine commitment to digital value protection sends a powerful message to the organization. Their actions, not just their words, define the cultural tone. By prioritizing digital value protection investments, participating in digital value protection training, and holding employees accountable, leaders create a culture where digital value protection is a business imperative.

Building a robust digital value protection culture is a journey, not a destination. It requires continuous effort, adaptation, and measurement. Organizations must invest in employee training, awareness programs, and communication channels to reinforce digital value protection messages. Regular cultural landscape assessments can help identify improvement areas and measure initiatives' effectiveness.

While technology is undoubtedly a crucial component of digital value management, culture determines organizational resilience to cyber threats. This holistic approach is essential in today's complex threat landscape, where the human element remains a primary target for adversaries.

Investing in a robust digital value protection culture is not just a compliance exercise; it's a strategic decision that can protect organizational reputation, financial stability, and competitive advantage. It's an investment in the future, where trust, integrity, and resilience are the cornerstones of success.



Final Thoughts

The traditional cybersecurity paradigm often focused on thwarting external threats, is increasingly insufficient in today's digital age. As organizations navigate the rapid evolution of technology, they must shift their perspective from merely protecting assets to actively leveraging digital capabilities to drive and preserve the quality and reliability of digital business value. Organizations can position themselves for long-term success in today's rapidly evolving digital landscape by adopting a digital value protection approach. By recognizing the strategic potential of digital value and aligning it with broader business objectives, organizations can create a secure, resilient, and innovative environment that drives value and growth. Organizational leadership must embrace several fundamental principles to transition the narrative from cybersecurity to digital value protection, including:

- **Establish a Vision:** Leaders must have the skills to establish a vision for digital transformation that prioritizes digital value protection.
- **Cultivate a Culture:** Leaders can cultivate a culture of digital responsibility by communicating the importance of digital value and its impact on the organization's overall success.
- **Empower Employees:** Employees should be empowered to contribute to developing, maintaining, and innovating digital systems. By involving employees in the process, organizations can foster a sense of ownership and encourage a proactive approach to protecting digital value.
- **Invest in Training:** Organizations must invest in training and development to ensure employees have the skills and knowledge to manage digital value protection effectively. This includes staying current with emerging threats, best practices, and technologies.
- **Foster Collaboration:** Communication and collaboration across departments and functions are vital for protecting the value of digital business. By breaking down silos and fostering open communication, organizations can identify and address potential vulnerabilities more effectively.

- **Prioritize Risks:** Digital risks should be evaluated based on their potential impact on business objectives, and investments in security measures should be prioritized accordingly.
- **Leverage Data:** Data-driven decision-making is essential. By leveraging analytics and metrics, organizations can measure the effectiveness of their digital value protection initiatives and identify areas for improvement.
- **Embrace Innovation:** Continuous improvement and innovation are essential. Digital value protection is an ongoing process, and organizations must invest in ongoing training, education, and technology to ensure the effectiveness of their digital risk mitigation measures.
- **Consider the Customer:** Digital value management should not be viewed in isolation. By considering the customer's perspective, organizations can ensure that their digital value protection measures do not compromise usability or create unnecessary barriers.

Learn more about helping your organization create a culture capable of creating, protecting, and delivering digital value by visiting www.dvmsinstitute.com



Improve your Cybersecurity Culture with the **Cybersecurity Cultural Assessment Tool (DVMS-CAT™)**

***Even today, human error is still the #1
cause of cyber-attacks and breaches***

One of the best ways for an organization to reduce cyber risk is to build a positive cybersecurity awareness culture. This entails creating a mindset in employees that the risk is real and their daily actions impact that risk.

The Cybersecurity Culture Assessment Tool (DVMS-CAT™) a comprehensive 67 question survey designed to understand employees attitudes and perceptions towards cybersecurity matters

Once results have been obtained, the tool's corresponding report provides actionable insights and advisable next steps, so your organization can best protect their digital business value.

For more information, go to **tools.dvmsinstitute.com**

Or,

Email: dvms@tso.co.uk

Tel: [+44 \(0\)1603 385601](tel:+44(0)1603385601)