WHITE PAPER

Leading with security

Essential insights to cultivate security as a core organizational value

LUMEN®

Table of contents

LUMEN®

Introduction

Organizational leaders face a complex matrix of security challenges that impact every facet of operations. As threat actors' attacks become more sophisticated, leaders must anticipate, respond and adapt like never before.

Security is the foundation upon which the pillars of modern organizations are built. It is a strategic priority that, when effectively prioritized, fosters an environment where predictability and reliability can flourish.

This white paper discusses essential insights relevant to cultivating security as a core organizational value. From silent threats that erode data integrity to a comprehensive security strategy, we present a blueprint for organization leaders to cultivate a security-first culture that not only defends but enhances business agility and innovation.

Security as a core value

The concept of security evokes images of shadowy figures orchestrating data breaches from behind a bank of monitors, along with sophisticated tools designed to protect our most sensitive information. It's a narrative dominated by the ongoing battle between cyber criminals and the tools developed to thwart them. However, this limited perspective fails to capture the full range of what security entails for today's businesses.

Security, when considered a core value, means you can be confident that things will go as expected, but if something does happen, you have the resources to quickly resume business as usual while minimizing damage.

By focusing on security as a core value:

- Customers know exactly what to expect from you, and they will trust that you will take care of their data, their reputation, and their future.
- Your ability to innovate is bolstered through a secure environment that allows for more calculated risks and exploration of new technologies.
- You are better suited for planning and decision-making given the reduced likelihood of unforeseen scenarios or lack of action plans.
- Partners and stakeholders have increased confidence in your operations, fostering stronger and more collaborative relationships.
- Your financial performance benefits from increased customer loyalty and reduced costs associated with incidents.
- Employee morale and productivity soar as a secure workplace promotes a safe working environment.

The pursuit of security as a core value transcends the confines of the cybersecurity portfolio. It's not a jigsaw puzzle to be completed with pieces solely from the cyber realm. Instead, it demands a holistic strategy integrating networking, edge fabric, and the rest of your operating capabilities. Together, these elements create a robust organization, safeguard data, and enhance customer relations for strategic success.

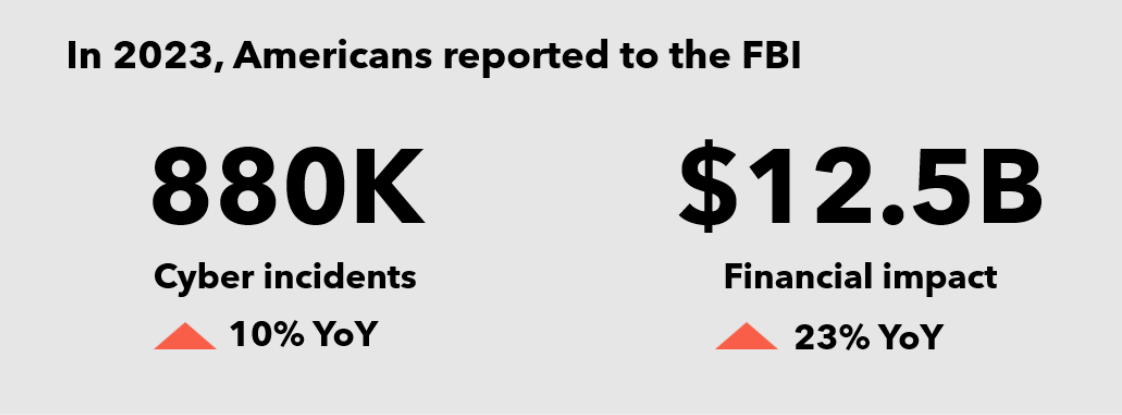
As a core value, security is inherently connected to predictability and reliability. From that perspective, risks extend beyond cyber-attacks and data breaches and require comprehensive solutions that place security at the forefront.

Silent threats and overt disruptions

Technological progress boosts efficiency, cuts costs, and raises productivity for organizations, but it also introduces new risks. The rise of Artificial Intelligence (AI) and Large Language Models (LLMs) is a current example of this duality. Bad actors are advancing their AI skills, adding deep fakes, and sophisticated social engineering campaigns to the threat landscape. Let's examine the current threat landscape and examine how these emerging risks are reshaping security boundaries.

An overview of the current security threat landscape

2023 marked a significant escalation in cybercrime. The FBI's latest Internet Crime Report revealed that Americans reported 880,000 cyber incidents with a staggering financial impact of $12.5 billion for the year, representing a 23% increase over 2022.[1] Echoing this concern, the White House's recent cybersecurity posture report highlighted that nation-state adversaries are intensifying their cyber capabilities at an unprecedented rate and, finding new ways to disrupt U.S. critical infrastructure.[2] This rise in cybercrime underscores the need for advanced and proactive measures to shield security perimeters.



Ransomware-as-a-Service

Tactic where bad actors franchise malware, allowing other criminals to use it in their ransomware attacks

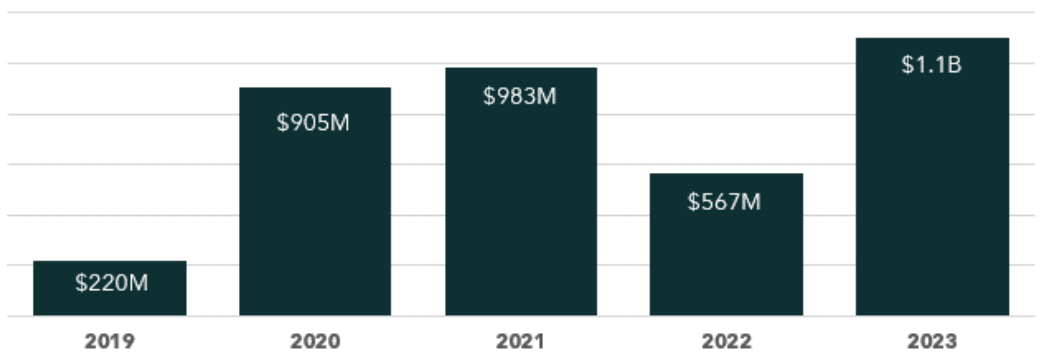
With the financial impact of cybercrime on the rise, it's crucial to turn our attention to the methods that are driving these numbers upward. Ransomware's toll reached new heights in 2023, with payments surging to $1.1 billion – nearly double the previous year's figures.[3] This alarming trend is partly fueled by the continued proliferation of familiar tactics, such as Ransomware-as-a-Service (RaaS) models, and new tactics like using Artificial Intelligence (AI) to increase attack sophistication and avoid detection.[4]

As ransomware continues to drain financial resources, we must also acknowledge strategic shifts in cyberattacks. Hybrid work models are shifting the cybersecurity battleground. Attackers now bypass traditional defenses by targeting small businesses and home office routers, creating backdoors into larger organizations. In 2023, the Black Lotus Labs® team by Lumen discovered the Cuttlefish malware – a

good example of this type of attack. This sophisticated malware was a significant advancement in data theft attacks. It didn't just sit silently and steal authentication credentials from networking devices – it also hijacked DNS and HTTP traffic on connections to private IP spaces. Its latest iteration targeted cloud-based resources to steal credentials and create a pathway to those assets through the affected device, making it appear like a legitimate login from a trusted device. The proactive measures of Black Lotus Labs have thwarted Cuttlefish by blocking its traffic across the Lumen global network.[5]

Figure 1

Total value received by ransomware attackers, 2019-2023.



Source: Chainanalysis[3]

The cybersecurity landscape is undergoing a rapid and complex transformation. In response to these evolving threats, it is imperative for businesses and government entities to remain alert and adaptable. Investing in cutting-edge security measures, embracing comprehensive and integrated solutions, and cultivating a culture that prioritizes security are no longer optional—they are essential to withstand the sophisticated challenges of today's digital world.

Invisible risks that compromise data integrity

Data is the cornerstone of modern business operations. It is harnessed to inform strategic decisions, drive customer engagement, and foster innovation. From tracking consumer behavior to optimizing supply chains, data insights enable businesses to operate efficiently and stay competitive. Having accurate, reliable data is essential for maintaining trust with customers, ensuring regulatory compliance, and achieving long-term growth.

Security risks go beyond cyberattacks and bad actors.

Due to its critical importance, data is under constant threat from cybercriminals, and their motives are diverse. Some profit from selling stolen data on black markets and the dark web. Others use it for political and social reasons, as evidenced in the Russia-Ukraine conflict, where data was sought for military advantage and espionage.[6] This kind of conflict can even impact private organizations, as in the case of Microsoft, which reported that Russian hackers stole their source code and continue to gain unauthorized access for spying.[7]

Unlike visible threats that can be quickly addressed, many cyberattacks remain hidden, allowing attackers to infiltrate systems for extended periods. And these undiscovered and long-term threats are especially dangerous. According to the Ponemon Institute, it takes 204 days for most companies to discover a breach.[8] Advanced Persistent Threats (APTs) can remain hidden in systems for months or sometimes even years, gradually collecting sensitive information. The longer these threats go undetected, the more damage they can inflict, undermining both data integrity and business operations.

Security risks aren't just about cyberattacks or hackers. Data integrity can be compromised by other factors including human error, data transfer errors, physical damage to devices and compromised hardware. Issues can also arise from a **lack of data integration, limited bandwidth, reliance on legacy systems and inefficient network architectures.** If these issues are not found and fixed with solid rules and systems in place, they can stay hidden and cause significant data integrity issues in the future.

Recognizing and addressing these invisible risks is critical to safeguarding your organization's data. By understanding the sophisticated techniques cybercriminals employ and the potential impact of human errors and infrastructure performance on data, organizations can implement stronger security measures to ensure data protection and resiliency.

Security as the bedrock of modern business

Security today requires more than just firewalls and encryption. A holistic security posture creates an environment that fosters four key elements of success and growth: reliability, availability, collaboration, and productivity.

Figure 2

Security as an optimization enabler

Let's explore how approaching security as a core value can help safeguard operations and protect your reputation.

How security safeguards operations

Standard operations are critical to any organization as they define how value is delivered to customers, users, and stakeholders. When streamlined, they can lead to cost savings, faster delivery times, and higher product quality—which gives the company a competitive edge in the market and enables it to scale.

Security events, however, can disrupt these operations. To combat this threat, the most successful organizations. deploy a comprehensive security approach that combines efficient solutions and advanced cybersecurity measures, while leveraging experienced talent.

Holistic security solutions include cybersecurity tools that extend throughout the networking architecture to protect against disruptions that could impact operational continuity.

Content Delivery Network (CDN)

Network of interconnected servers that enhance application performance

Distributed Denial-of-Service (DDoS) Mitigation service

Service that protects digital environments against single and multi-vector attacks.

Secure Access Service Edge (SASE)

Framework that combines network and security capabilities into a single, cloud-delivered platform.

A financial institution safeguards its operations with backup servers for essential records and data. It uses SD-WAN for efficient branch connectivity and has disaster recovery plans in place. Additionally, it employs a third-party service for continuous management, allowing swift recovery from system failures or attacks, minimizing customer impact.

An e-commerce firm employs edge computing and robust security measures for rapid content delivery and data safety. It uses a CDN and DDoS mitigation to protect services. It also displays security certificates on its website confirming the safety of customer information and fostering trust and loyalty.

A city's Public Works Department adopts SASE for secure, low-latency connections to critical resources. It uses access control systems to protect sensitive areas such as water treatment plants, and edge fabric to process data closer to the plants. It also deploys cybersecurity tools and disaster recovery plans to provide continuity of services during emergencies.

How security protects reputation

Reputation is a critical asset for any organization. It can take years to establish and only minutes to destroy. Security incidents such as data breaches or operational disruptions can severely damage a company's standing with customers, partners, and the public.

> Publicly traded companies suffered an average decline of 7.5% in their stock values after a data breach. [9]

The genetic testing company 23andMe reported a data breach in late 2023 that compromised the personal data of roughly 7 million people as cybercriminals sold customers' names, addresses, and heritage information on the dark web. This case was highly public at the time, not only because of the implications of the data breach and the impact on millions of customers, but also because the company tried to blame customers for the incident.[10]

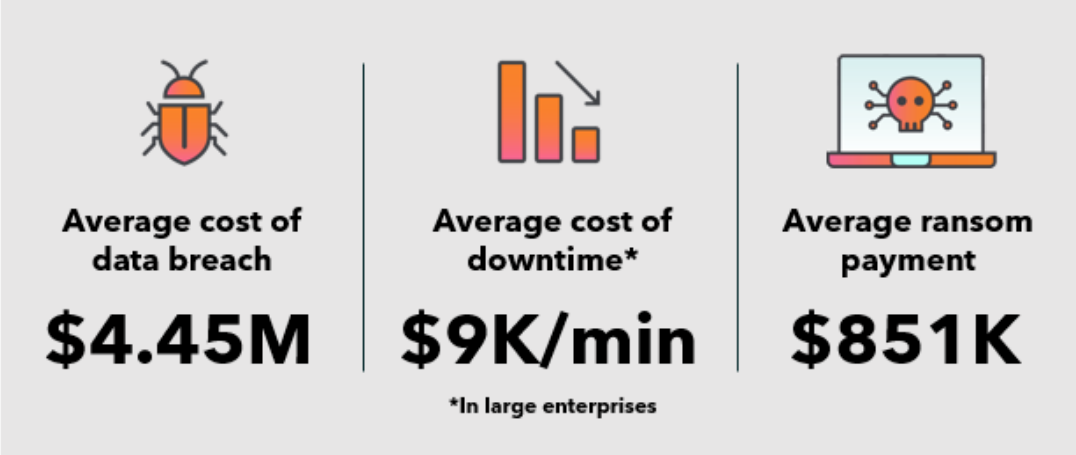
A proactive, holistic, and reliable security strategy anticipates multiple scenarios where operations or data could be compromised. It also demonstrates to stakeholders that the organization takes its responsibilities seriously, and it builds trust by showing a commitment to protecting sensitive information and the reliability of services.

In the event of a security incident, effective communication is crucial. Transparency can mitigate reputational damage and reassure stakeholders of the organization's integrity and responsiveness.

The financial impact of weak security posture

With complex network structures, talent scarcity, and a rapidly evolving threat landscape, organizations struggle to overcome risks and ensure seamless operational continuity. The inevitable question in every organization is not *if* a security incident will strike – it's *when*, and are they prepared to respond effectively?

Costs associated with cyberattacks are on the rise. The Ponemon Institute reports that data breaches cost on average $4.45 million[8], large enterprises lose about $9,000 per minute during downtime[11], and the average ransom payment is $850.700.[12] But the impact does not stop there. Multiple processes and operations are impacted during any given incident. Customer service channels could see spikes in customer calls, internal teams will need to shift their focus to issue resolution, and legal teams may need to engage in compliance and litigation efforts.



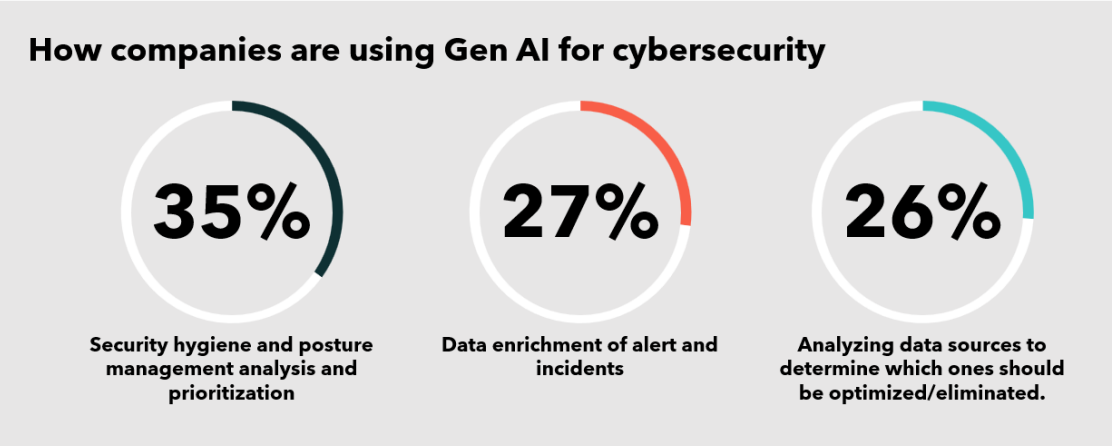
The need for robust security measures is clear. The stakes are high, and the costs of inaction are even higher. As we've seen, the financial repercussions of incidents are substantial, and the ripple effects extend far beyond the immediate financial loss. This is why a strong security posture is a shield against threats and a strategic asset that can enhance operational efficiency, foster customer trust, and differentiate a brand in a crowded marketplace. Investing in security is investing in the future – a future where resilience becomes a competitive advantage, and preparedness is synonymous with success.

The business case for security is a narrative of defense, and a story of empowerment and opportunity in the digital age.

Security and artificial intelligence

Artificial Intelligence (AI) is swiftly becoming essential in many sectors, driving innovation and shaping the future of work. Recognizing the transformative potential of AI, numerous organizations are launching enhanced applications and investing heavily in AI-driven systems. A recent IDC survey revealed that 37.4% of respondents reported that "Generative AI will disrupt their competitive position"[13], emphasizing the need to embrace this technological evolution.

AI has also begun to revolutionize security. It bolsters defenses with cutting-edge, real-time threat detection and automated responses. Its rapid analysis of vast data sets allows organizations to anticipate and mitigate potential threats. AI also streamlines the compliance process by continuously monitoring and enforcing regulatory standards, reducing the risk of human error and regularly updating security measures with the latest regulations. Additionally, AI can simulate various attack scenarios, helping to develop robust security protocols and train cybersecurity professionals.



Source World Economic Forum[14]

Optimizing operations with AI

By integrating AI into cybersecurity strategies, organizations can automate and enhance various security operations, freeing their resources to focus on strategic imperatives as they improve their security posture. Some of the applications are:

- **Enhanced decision-making:** AI can analyze trends and patterns to forecast potential security incidents. This analysis aids in prioritizing security measures and allocating resources efficiently. Such foresight is essential for predicting future events, improving decision-making, and enhancing resilience and proactive responses.

- **Operational efficiency:** Real-time, automatic threat-detection systems empower AI algorithms to identify potential threats swiftly and precisely. This speed in analysis lessens the reliance on manual monitoring, freeing staff to concentrate on strategic tasks. Consequently, businesses become more efficient and can maintain their growth trajectories without interruption.

Rapid Threat Defense, the Lumen automated threat detection and blocking feature, is updated with AI-enhanced threat intelligence from Black Lotus Labs every 15-30 minutes to protect the Lumen network.

- **Improved customer satisfaction:** AI streamlines network solutions by optimizing data flow. It analyzes real-time traffic, peak periods, and bottlenecks, then adjusts routes and bandwidth to improve speed and reduce congestion. Intelligent traffic management helps ensure critical applications get necessary bandwidth, thus elevating the user experience and customer satisfaction.
- **Streamlining compliance and governance:** The automation of regular security tasks has been widely adopted as AI takes over log analysis, incident response, and policy enforcement. This shift allows security staff to focus on strategic planning, helps maintain consistent compliance, and reduce the risk of human error.

An example of this application is **Lumen Defender,** which proactively blocks threats based on customers' risk tolerance, with easily customizable alerts and deny/allow lists to further automate tasks.

- **Boost productivity:** AI helps to differentiate between real threats and benign anomalies, which can minimize disruptions from false positives. This focus allows security teams to address actual threats more efficiently, enhancing response times and productivity.

- **Increase operational uptime:** AI can minimize downtime by predicting network or fabric equipment failures before they occur. This process includes continuous monitoring and analysis of data from the equipment, such as temperature readings, performance metrics, error messages, and historical failure patterns. It helps ensure operations run smoothly.

Mitigating AI-related risks

As organizations increasingly integrate artificial intelligence (AI) into their operational fabric, the imperative to shield AI-powered systems from advanced threats grows ever more critical. Consider some of these risks:

- **Operational disruption, unreliability, and compromised data integrity:** With AI integration comes the increased risk of data poisoning. In 2024, the National Institute of Standards and Technology (NIST) underscored the perils of adversarial machine learning,[15] such as attackers manipulating AI to induce malfunctions. To combat these threats, organizations need to enforce stringent data validation, persistent monitoring, and regular retraining to maintain the integrity of their AI systems.
- **Loss of competitive advantage and intellectual property:** The theft of proprietary AI models can lead to their unauthorized use or resale, resulting in financial losses and a reduced market share. As the value of AI models increases, the threat of intellectual property theft looms larger. Watermarking and encryption are vital to defend against the misuse of proprietary models.[15]
- **Loss of trust and confidence:** AI threat landscapes are in constant flux. The recent unearthing of malevolent models on platforms like Hugging Face underscores the potential weaponization of AI.[16] Attackers exploiting these models could run arbitrary code on devices, breaching security and disrupting business operations. Staying abreast of emerging threats and deploying sophisticated threat detection is crucial to swiftly identify and mitigate such risks.

Figure 3

The dual nature of AI in security

Defense

AI-driven predictive and behavioral analytics have greatly enhanced threat detection, allowing for proactive defense measures. An example of this is how Lumen leveraged its exceptional network visibility and Lumen Black Lotus Labs' advanced machine learning algorithms to identify Qakbot infections –a major banking trojan - up to 3 days earlier than public threat feeds.

Offense

Recent incidents, like the Hong Kong deepfake scam, demonstrate how AI can be used maliciously. In this case, scammers used deepfake technology to impersonate a company's CFO, leading to a fraudulent transfer of $25 million. Every person on the video conference call was a deepfake, tricking the employee into believing the original phishing message he received from his supposed CFO was legitimate. This is just one example of how AI can enable attacks that are faster, smarter, and more powerful.

Security challenges in the public sector

Public sector agencies prioritize maintaining public trust and ensuring the continuity of essential services. They also focus on protecting citizen data and meeting regulatory standards. Despite this, budget constraints and complex procedures delay their adoption of new technologies, leading to a cautious security approach. This emphasis on compliance and service protection may slow their response to new security threats but helps ensure comprehensive risk management and legal compliance.

In general, agencies face a broader spectrum of security threats than private businesses. They encounter common threats such as cyber-attacks, and also unique challenges tied to their public service operations. Stringent regulations and the risk of disruptions from outdated technology or limited resources add layers of complexity. Below are some examples:

> Public Sector agencies often struggle with the challenge of protecting sensitive data and ensuring compliance with stringent regulatory frameworks while contending with the limitations of legacy technology.

Risks shared with private sector: Agencies are increasingly targeted by malicious activities such as denial-of-service attacks, ransomware, and phishing. These incidents carry significant consequences:

- **Operational disruption:** The availability of critical services essential to public welfare and national safety. Similarly, healthcare systems under attack are unable to provide quality patient care, which could lead to fatal consequences.
- **Reputational damage:** After being attacked, agencies can experience a severe decline in public trust, leading to heavier regulatory oversight, and even resulting in shifts in domestic or international policy.
- **Financial loss:** Public entities often lack the robust financial buffers of private businesses, leading to longer recovery times and potential increases in public spending.

Risks associated with government operations: Public agencies handle sensitive data and critical infrastructure, making them appealing targets for adversaries looking to disrupt governmental operations or gain access to confidential information. Risks increase when state-sponsored actors use advanced tactics to infiltrate agencies' networks, like in the cases below:

- **Tactics of foreign malign influence operations:** Cyber adversaries could manipulate elections voter registration systems, ballot counting software, or other election-related processes to alter outcomes. This form of interference can

undermine the democratic process and has been a concern in various countries. In response, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has released guidance on securing election infrastructure against tactics of foreign malign influence operations, highlighting the complexity of threats and the need for robust security measures.[17]

- **User data exploitation and surveillance:** Applications with large user bases can be exploited for mass data collection, leading to concerns about user privacy and national security. Platforms like TikTok have faced scrutiny for their potential to allow foreign governments to track and collect user data for espionage purposes.[18]
- **Cyberterrorism and theft of classified information:** Driven by political or ideological purposes, cybercriminals and nation-state actors could use the internet to threaten, cause harm, or exploit system vulnerabilities and access to classified information.
- **Budget and staffing limitations:** Public administration's financial constraints often limit the adoption of advanced security technologies and proper personnel training, impacting the ability to respond to security threats. Moreover, the scarcity of talent disproportionately affects government agencies, as they struggle to match the private sector's competitive salaries.[19]
- **Legacy system vulnerabilities:** Public sector organizations often rely on outdated legacy systems, which can be more vulnerable to security threats and create challenges for integrating with next-gen technologies, ultimately increasing the risk of security breaches.

Cultivating a security-first culture

Cultivating a security-first culture within organizations has become a critical defense against persistent threats. The advantages of this approach are clear and compelling: it minimizes the impact of cyber threats, builds customer trust by demonstrating a commitment to privacy and security, and enhances compliance with various regulations and standards.[20]

Innovation thrives in environments where risks are managed effectively, and security-first cultures provide a framework where new ideas can be assessed and implemented with reduced risk. Organizations can explore innovative solutions to enhance services and citizen engagement by making sure new technologies and processes are built securely from the start.

Still, many organizations struggle to maintain optimal security measures adapted to the ever-evolving threat landscape, as evidenced below:

- Human errors account for 95% of security breaches, yet only 3% of IT security spending is allocated to security training.[21]
- Forbes reports that many organizations rely on basic security training, making them vulnerable to modern, sophisticated cyber threats.[22]
- 30% of employees do not believe they play an active role in their company's cybersecurity posture, and only 39% are likely to report a security incident.[22]

These statistics underscore a critical gap in security: the human factor. A security-first culture is vital, and it requires every member of the organization, from the CEO to the intern, to make security an ever-present priority. Investing in frequent and up-to-date employee training is essential, as it strengthens the organization's defenses and turns potential weaknesses into strong points:

For mid-sized organizations, this means embedding security considerations into the growth strategy to protect new investments and initiatives.

Large enterprises must navigate a complex web of security risks, making a security-first culture essential for defending against threats that can disrupt operations and impact the bottom line.

Public sector agencies that manage sensitive public data must ensure security is integrated throughout their systems, processes, and training so they can maintain public trust and comply with regulations.

When security is prioritized, organizations can innovate with confidence.

In the public sector, a security-first culture does more than shield against risks — it propels agencies forward. The World Economic Forum points out that cyber resilience is a key priority for agencies because it enables them to effectively deliver services in an unpredictable world.[23] With a security-first approach, agencies can embrace digital transformation and innovation while upholding the public trust and meeting the expectations of a digitally aware public.

In conclusion, promoting a security-first culture is more than a strategic choice – it is a critical necessity. By embedding security into the core of organizational culture, enterprises and agencies alike can achieve their strategic goals while upholding the highest standards of security vigilance and resilience.

A comprehensive security strategy

Effective security frameworks extend past the traditional defenses, encompassing sophisticated threat detection systems, state-of-the-art solutions, and an integrated perspective that helps ensure robustness, dependability and efficiency. Below is a list of key elements you should consider embracing security as a core organizational value:

A holistic security strategy starts with:

- **High-speed, dedicated, secure, and reliable network connectivity** to improve operational efficiency, security, and communication through flexible bandwidth that scales with operation needs and provides the necessary capacity to operate efficiently.
- **Networking and application protection solutions** that help organizations monitor their digital assets for signs of suspicious activity and automatically identify and block potential threats before they cause harm. Products in this category include SASE, DDoS Mitigation Services, Edge application protection and acceleration, and perimeter security. Robust, holistic web protection is critical to strengthen online presence and protect bandwidth, -which is essential to maintain connectivity- and application performance.
- **Regular security training and awareness programs**: Human error remains the leading cause of security breaches. By educating employees about common threats such as phishing and social engineering, organizations can reduce the likelihood of a successful attack.
- **Protection and encryption of data** in transit and at rest ensures its security even if it is intercepted or accessed by unauthorized parties. Data loss prevention (DLP) solutions monitor and control the movement of sensitive data, preventing accidental or malicious leaks.

And a holistic strategy expands to the following components:

- **Ongoing management –** including regular updates, patches, and performance monitoring – helps maintain system integrity and efficiency and reduces the likelihood of failures and downtime.
- **Performance optimization** through continuous monitoring and improvement of IT infrastructure. Performance management tools track system metrics and user experiences, identifying bottlenecks and areas for enhancement. By ensuring that systems operate at peak efficiency, organizations can deliver consistent, high-quality services to their customers and stakeholders.
- **Advanced threat detection and response** from solutions such as intrusion detection systems (IDS) or security information and event management (SIEM) systems to provide real-time monitoring and analysis of events. These systems use sophisticated algorithms and machine learning to identify unusual patterns and behaviors that may indicate a security breach, enabling swift response to contain and mitigate threats.
- **Advanced Threat Intelligence** to help proactively identify, understand, and mitigate potential threats, vulnerabilities, and attacker methods. This information is essential for preparing robust and flexible strategies, improving incident response capabilities, minimizing the impact of successful breaches, and effectively protecting assets and sensitive data.
- Developing and regularly updating an **incident response plan** that outlines clear procedures for identifying, containing, eradicating, and recovering and ensures that the organization is prepared to handle events effectively.

Conclusion

Security is more than just firewalls and VPNs; it's a fundamental value that underpins an organization's success. When security is considered a core value, it builds trust among customers, partners, and employees, fostering a stable environment conducive to growth. Embracing this approach to security encourages innovation and smart risk-taking within a protected framework. It leads to better planning and decision-making, as it minimizes unexpected events and helps ensure preparedness. It also translates to financial gains by cutting costs related to breaches and earning customer trust.

Organizations pursuing security as a core value require a holistic strategy that integrates networking, edge fabric, and all operating capabilities, empowering them to protect data through seamless and secure operations, enabling better customer experiences and strategic achievements.

How Lumen enables security

Lumen takes a holistic approach to security by building it into the solutions and services we provide. These solutions can be integrated with your existing infrastructure to safeguard your data and applications, ultimately enhancing customer experience. Backed by a comprehensive security approach and the skills and expertise required to design, implement and manage these solutions, Lumen assists organizations in securing their applications and valuable data and creating a security-first culture.

Partner with Lumen to

- Streamline your **network** experience with cloud-like flexibility, scalability, and built-in cybersecurity.
- Safeguard your applications, critical data, and digital landscapes with our top-tier **cybersecurity** solutions.
- Stay agile and reliable with a dynamic and secure **network** that adjusts to your demands in real time.
- Enhance availability and capacity for cutting-edge applications and data processes through our advanced **edge fabric** infrastructure.
- Accelerate and secure your transformational journey by teaming up with our **seasoned experts** who will guide you every step of the way.
- Foster innovation by allowing your team to concentrate on strategic initiatives, while our **specialists handle the operational complexities**.

About Black Lotus Labs

BLACK LOTUS LABS

We see more, so we can stop more

Black Lotus Labs is Lumen's threat intelligence team who specializes in detecting, tracking and disrupting threats around the world.

Keeping Lumen and our customers safe

200B+ NetFlow sessions monitored daily.

We track **~2M threats per day** providing us with a comprehensive understanding of the global threat landscape.

Execute over **~150 disruptions** per month through takedowns and notifications.

Contact us and learn more about how Lumen's solutions and capabilities can benefit your organization today.

LUMEN®

Footnotes

[1] Federal Bureau of Investigation, Internet Crime Report 2023, April 4, 2024 - Link
[2] The White House, Fact Sheet: 2024 Report on the Cybersecurity Posture of the United States, May 07, 2024 - Link
[3] Chainanalysis, Ransomware Payments Exceeded $1 Billion in 2023, Hitting Record High After 2022 Decline, Feb 7, 2024 – Link
[4] National Cyber Security Center (NCSC), The near-term impact of AI on the cyber threat, Jan 24, 2024 - Link
[5] Black Lotus Labs, Eight Arms To Hold You: The Cuttlefish Malware, May 1, 2024 -Link
[6] Dark Reading, Europe Sees More Hacktivism, GDPR Echoes, and New Security Laws Ahead for 2024, Dec 26, 2023 – Link
[7] Center for Strategic and International Studies, Significant Cyber Incidents - Link
[8] IBM and Ponemon Institute, Cost of Data Breach Report 2023
[9] Harvard Business Review, The Devastating Business Impacts of a Cyber Breach, May 04, 2023 - Link
[10] The Guardian, Hackers got nearly 7 million people's data from 23andMe. The firm blamed users in 'very dumb' move, Feb 15, 2024 – Link
[11] Forbes, The True Cost Of Downtime (And How To Avoid It), Apr 10, 2024 - Link
[12] Coveware, Scattered Ransomware Attribution Blurs Focus on IR Fundamentals, Oct 30, 2024 - Link
[13] Jyoti, Ritu; IDC, Embracing the AI-Driven Paradigm Shift, Jun 5, 2024
[14] World Economic Forum, Cybersecurity is on the frontline of our AI future. Here's why, Jan 15, 2024 - Link
[15] National Institute of Standards and Technology, Adversarial Machine Learning, Jan 2024 - Link
[16] Dark Reading, Hugging Face AI Platform Riddled With 100 Malicious Code-Execution Models, Feb 29, 2024 - Link
[17] CISA, CISA, FBI, and ODNI Release Guidance for Securing Election Infrastructure Against the Tactics of Foreign Malign Influence Operations, Apr 17, 2024 - Link
[18] CSIS, TikTok and National Security, Mar 13, 2024 - Link
[19] World Economic Forum, Strategic Cybersecurity Talent Framework, April 2024 -Link
[20] ISACA, Building a strong security culture for resilience and Digital Trust. (n.d.) – Link
[21] CyberPilot, Hofmann, S. The Ultimate Guide to a strong security culture, Jan 24, 2024 – Link
[22] Forbes, Gilliland, A. Council post: Building a security-first culture: The key to cyber success, Jan 4, 2023 – Link
[23] ISACA, An executive view of key cybersecurity trends and challenges in 2023, Aug 22, 2023 - Link

*This content is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. Lumen does not warrant that the information will meet the end user's requirements or that the implementation or usage of this information will result in the desired outcome of the end user. This document represents Lumen products and offerings as of the date of issue

Why Lumen?

Lumen is your single provider to enable digital transformation. With a comprehensive portfolio and experienced talent, we can help safeguard customer experience, protect your confidential data, and manage threats your business could face. Backed by the extensive and deeply peered Lumen global network, Black Lotus Labs' threat intelligence, and our team of security experts with the skills and experience to deliver, Lumen is a trusted partner to help you strengthen your security posture.

866-352-0291 I lumen.com I info@lumen.com

LUMEN®