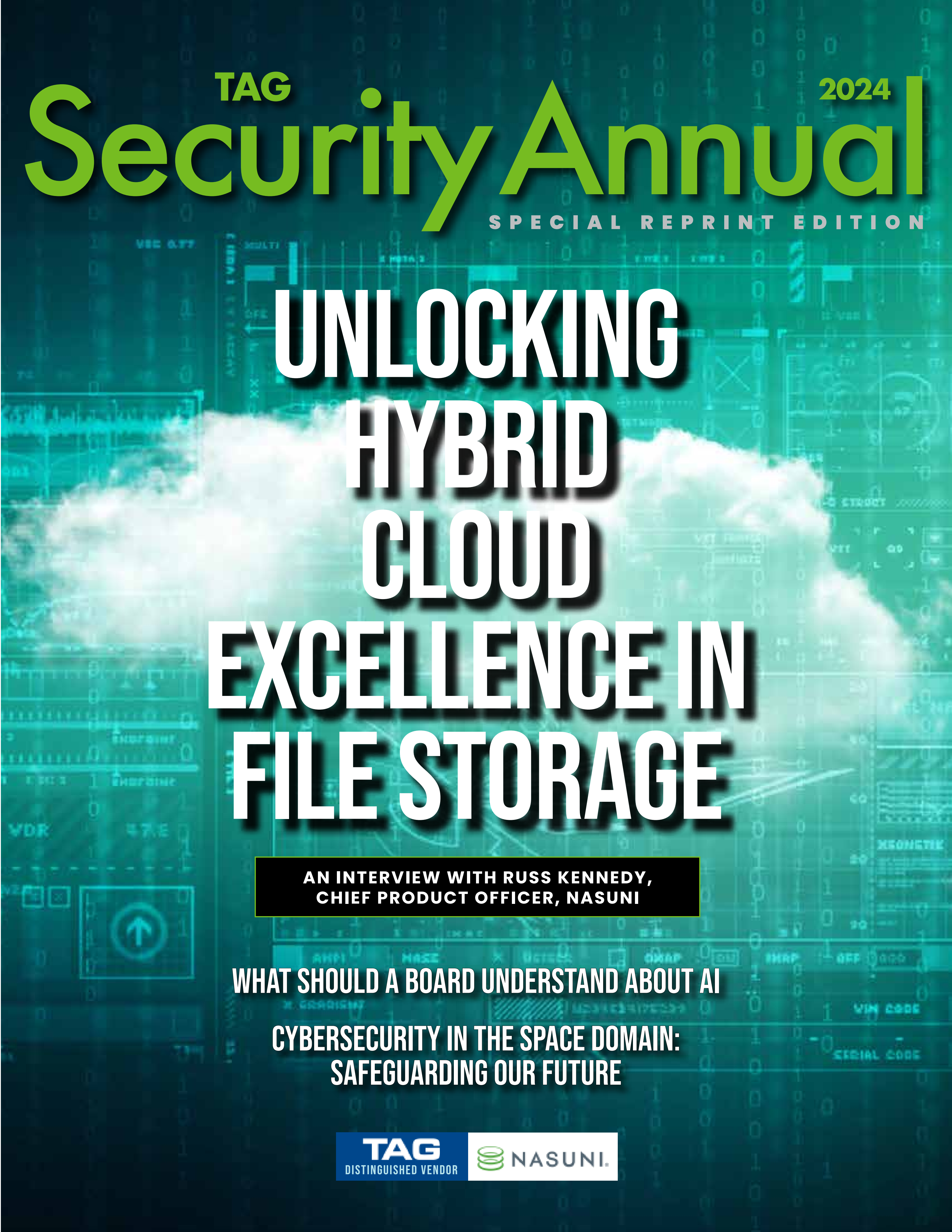
TAG Security Annual 2024

SPECIAL REPRINT EDITION



UNLOCKING HYBRID CLOUD EXCELLENCE IN FILE STORAGE

AN INTERVIEW WITH RUSS KENNEDY, CHIEF PRODUCT OFFICER, NASUNI

WHAT SHOULD A BOARD UNDERSTAND ABOUT AI

CYBERSECURITY IN THE SPACE DOMAIN: SAFEGUARDING OUR FUTURE

TAG DISTINGUISHED VENDOR

NASUNI

The need to reduce cyber risk has never been greater, and Nasuni has demonstrated excellence in this regard. The TAG analysts have selected the Nasuni Corporation as a 2024 Distinguished Vendor, and such an award is based on merit. Enterprise teams using Nasuni's platform will experience world-class risk reduction—and nothing is more important in enterprise security today.

The Editors,
TAG Security Annual
www.tag-cyber.com

REPRINTED FROM THE TAG SECURITY ANNUAL

AN INTERVIEW WITH RUSS KENNEDY, CHIEF PRODUCT OFFICER, NASUNI

UNLOCKING HYBRID CLOUD EXCELLENCE IN FILE STORAGE

In the ever-evolving landscape of cybersecurity and hybrid cloud storage, Nasuni has emerged as a key player. Delving into their innovative approach, this Q&A explores how Nasuni addresses the shifting needs of businesses. From their unique security measures to ensuring a seamless transition, Nasuni sheds light on the future of hybrid cloud storage, offering valuable insights for organizations navigating this complex terrain.

TAG: Can you elaborate on how Nasuni's hybrid cloud storage platform stands out and addresses the evolving needs of businesses?

NASUNI: The era of file storage silos has ended. Relying on outdated infrastructures with isolated technologies at various locations no longer satisfies users or supports strategic business goals. Cloud-only solutions pose performance challenges. Nasuni's File Data Platform offers a hybrid cloud storage solution, surpassing traditional options. It breaks free from NAS limitations, enabling scalable storage, significant risk reduction, and lowered operating costs.

Nasuni is the preeminent hybrid cloud storage solution, excelling across three crucial value pillars. Effortless scalability allows on-demand provisioning of SMB and NFS file shares globally, managed seamlessly through Nasuni and object storage subscriptions. The high-speed read/write performance at the edge ensures a smooth transition without disrupting existing workflows. Nasuni offers unmatched data security, providing real-time ransomware protection, up-to-the-minute recovery points, and the ability to recover petabytes of data in seconds, all at the edge. This eliminates the need for backup or disaster recovery considerations for file data.

TAG: How does Nasuni ensure data security, including encryption, role-based access, and protection against hacking or compromise?

NASUNI: We see the worlds of security teams and the CISO coming together with the world of storage and infrastructure. A company's precious data, and more importantly, its file data, is often a target for hackers. Having cyber-storage capabilities built into whatever file data platform you use is a must.

With Nasuni, you get a platform with a robust security model that combines strong AES-256 encryption and local authentication with the native capabilities of top-tier cloud storage solutions such as Amazon Simple Storage Service (Amazon S3), Microsoft Azure Blob object storage, and Google Cloud Storage.

Nasuni offers ransomware detection for file activity, attack mitigation, and recovery support. Nasuni's ransomware solution detects attacks in real time and looks for known signatures and anomalous behavior that signify ransomware activity. These activities are immediately mitigated, and the recovery process can handle millions of files in minutes using a patented rapid recovery process based on dialing back an unlimited number of immutable snapshots.

With Nasuni, you get a platform with a robust security model that combines strong AES-256 encryption and local authentication with the native capabilities of top-tier cloud storage solutions.

In addition, Nasuni can help accelerate ecosystem-wide threat response posture via SIEM solutions like Microsoft Sentinel. Your SecOps team gets an early warning from edge detection to launch automated responses, perform investigations, and meet compliance requirements.

TAG: Traditional backup and recovery solutions often require significant hardware and software. How does Nasuni render traditional backup obsolete and provide faster and more precise ransomware recovery?

NASUNI: Conventional backup solutions require significant hardware and software to run a typical 3-2-1 data protection strategy. Replication strategies introduce substantial risk, and by the time a security breach is detected, the damage has spread across multiple backup copies. Recovery is often lengthy and problematic—extending downtime and impacting productivity.

Nasuni changes all that. You can recover entire volumes in minutes with infinite file versioning and immutable snapshots. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are measured in minutes to protect file data without additional backup software. These snapshots are unlimited, incorruptible, can be retained indefinitely, and stored in cloud object storage.

Regarding recovery from a disaster or an attack, Nasuni can recover millions of files in a minute since there is no need to move or restore any data—you simply "dial back" to a point before the attack occurred. Likewise, Nasuni lets you focus on restoring only affected files vs. an entire volume or folder – realizing even greater time efficiencies.

This recovery and detection at the edge is an important line of defense for any security stack with an advantage over traditional storage methods that rely on analyzing and recovering from completed backups.

TAG: Could you elaborate on how Nasuni ensures a seamless transition for businesses, allowing them to realize the scalability, security, and performance benefits without disruption?

NASUNI: A Nasuni migration process is a well-thought-out, thoroughly tested process trusted by hundreds of customers. The data movement from your legacy infrastructure parallels regular file access. The cutover to Nasuni happens quickly and easily—often a simple matter of remapping drive letters to point to Nasuni. Users are frequently unaware that migration has even occurred.

Your corporate data is your most valuable asset. Ensuring there's no opportunity for data loss or exposure is essential. The phrase "data loss" strikes fear in any IT professional, but there is no opportunity for data loss when moving to Nasuni.

Moving your global file-share platform to Nasuni will directly impact your bottom line thanks to the cost savings, unlimited scale, and significant performance gains.

TAG: How does Nasuni's architecture allow for greater AI/ML and data intelligence use?

NASUNI: Unstructured data locked away in storage silos represents a vast and underutilized asset for most companies. While traditionally viewed as a cost and compliance burden, this data can provide immense value when made available to AI systems. However, realizing this benefit requires transforming scattered storage silos stores into an accessible single–source–of–truth.

Companies relying on existing traditional file storage infrastructure, including Windows File Servers, Network Attached Storage (NAS), backups, and more, are not designed to handle the complexities of modern industry, artificial intelligence, or machine learning capabilities. With a hybrid cloud solution like Nasuni, organizations can consolidate, secure, and access their files in one shared global file system and deliver powerful new insights and visibility within the Nasuni File Data Platform. Administrators can quickly assess file data usage patterns, make proactive data management decisions, and better enable the delivery of intelligent insights.

Consolidating scattered and unstructured file data must be the foundation for an AI strategy. By migrating the disconnected contents into a unified file storage lake armed with consistent access permissions, metadata schemas, and governance, it's possible to tap into previously trapped insights, artificial intelligence, and machine learning capabilities to gain traction.

WHAT SHOULD A BOARD UNDERSTAND ABOUT AI?

DR. EDWARD AMOROSO

The governing role of the board member is generally well-defined, but often misinterpreted by observers. So let me start with a reminder of what corporate board members are expected to do. First, they must participate in reviewing and overseeing management. This requires the skill to know when and where to chime in, and this is easier said than done.

Second, they must participate in corporate strategy to help drive the company to an optimal decision when something truly consequential is being considered. Major mergers and acquisitions, for example, generally demand the attention of the board, but minor, day-to-day management decisions do not. Again, the principle sounds easy but sticking to it in practice is not..

Finally, corporate board members are expected to review and ensure the accuracy of important financial statements and other key data reported by the company. This does not imply using a fine-toothed comb to review every ledger item, but it does require active enough participation to ensure that public reporting is correct.

In addition to these responsibilities, board members frequently find themselves wading into new areas of concern that their companies confront. Cybersecurity is one such area that has spurred considerable debate about whether directors should play a significant role in making decisions, and if so, how involved they should be. Certainly, they are not expected to be security experts, but general agreement exists that broad awareness is now necessary.

A comparable issue involves artificial intelligence (AI). In recent months the public dialogue has been intense (to say the least). You can be sure there have been innumerable private conversations behind closed doors. What are AI's implications for the business? And by the way, how will it affect security? Just as corporate directors are not expected to be experts in that field, they are not expected to be experts in AI. But a consensus is emerging that it is a key aspect of a board's responsibilities.

That said, what are the key considerations for board members on this subject? What should they know about the business implications and security implications? How much do they need to understand about this important technology?

Business leaders will obtain guidance on future trends in the same way a radiologist can work with AI to view data and create accurate interpretations.

BUSINESS IMPLICATIONS

The effects of AI on business will differ from one industrial sector to another, but some general statements can be made. Hopefully, these broad characteristics in the context of modern business will start the intellectual process for board members to begin integrating AI-related impacts to their governing responsibilities.

Below I've listed issues with an emphasis on how they relate to boards. I've skipped over those that might have a substantial impact on business but not on board responsibilities. Please keep this in mind. My guidance here is for boards, not day-to-day executives and practitioners.

Business Writing Will Become Software-Defined

Board members should recognize that for many years the quality of normal business writing has varied considerably. I'm talking about the memorandums, policy statements, agendas, meeting minutes, and other narratives that have been used in business for decades.

The problem is that so much of this writing has been just terrible, often including nonsensical reports, lengthy papers, and unclear narratives. Board members are certainly familiar, for example, with the large volume of often unintelligible materials presented in advance of meetings. This is common across all aspects of modern business.

AI will have a direct influence on the quality of these written artifacts because automation is so well-suited to this task. Auto-generated notes after online meetings are already common, and this will extend to a fully software-defined approach to business writing that will have considerable consequence on all forms of business communications. And it should represent a tremendous improvement.

AI Will Drive Business Macro Trend Analysis

Board members and corporate executives have depended for many years on the predictions and observations of trends in the marketplace. These often come from industry analysts who opine based on their admittedly limited view of the many factors that influence any type of prediction.

While there will always be interesting personalities who can provide incisive and even humorous observations on macro trends, the use of AI to analyze market trends will be a more common occurrence. The advantage AI has is that it can include virtually every factor for which some evidence is available to drive the optimal prediction.

Board members should expect to see a symbiotic relationship between human and automated market trend analysis. Business leaders will obtain guidance on future trends in the same way a radiologist can work with AI to view data and create accurate interpretations.

The first obligation that every board member should recognize—and this point should be patently obvious—is that a basic working knowledge and baseline understanding of AI is a requirement for modern board members.

Customers Will Learn to Accept AI for Certain Applications

The ongoing debate with respect to the suitability and acceptability of using AI for certain applications will gradually wane in favor of societal acceptance of the technology. This happens for every new technological advance, including early industrial advances as well as the advent of computing.

The implications for board members is that aggressive adoption of AI, where appropriate, is the best course of action, and hesitation related to concerns about societal qualms is not recommended. Certainly, regulation and some degree of control will be required, but I advise businesses to be aggressive.

SECURITY IMPLICATIONS

The security implications for any type of business will involve offensive considerations ("Can we be hacked by an adversary using AI?") as well as defensive considerations ("Can we use AI to protect ourselves from an adversary?"). As one would expect, use of AI for both is an obvious corollary.

Below I lay out key security-related issues that emerge for board consideration. These should be addressed and coordinated across the entire management chain, and that should include the chief information security officer (CISO).

Major Adversaries Will Use AI to Attack

An important recognition that every business must understand is that their country of origin will certainly be targeted by nation-state adversaries using AI-based offensive measures. Organizations located in the United States, for example, should expect that countries such as China and Russia will most likely develop and use these methods.

The implication from a corporate perspective is that the front line for cyber threats is not the military or even the government, but rather is the distributed collection of data from business, enterprise, industrial groups, families, individuals, and other non-government targets. This is where an adversary nation will target with cyber threats.

Countries Will Need AI to Protect Infrastructure

Special consideration is obviously needed in protecting critical infrastructure, if only because the consequences of an attack can be so much more severe than attacks to other sectors. For board members with responsibility to manage critical and essential services, the need to maintain secure defenses against AI-based smart attacks will be paramount.

An implication of the existence of AI-based offensive cyber methods is that organizations will need AI-based defensive measures to put a reasonable protection in place. It should be obvious that if an automated attack is being levied, then the defender will not be able to stop such an attack merely by using manual, procedural methods.

Board members should be cognizant of major investments in AI-based security infrastructure, not to review or approve the specifics of the technology or vendors selected, but rather to ensure that a strategic plan is in place to maintain the ability to stop these new forms of attack with a solid AI-based protection scheme.

Social Engineering Will Benefit from AI

One attack that all board members will be familiar with involves the use of social engineering tactics to trick an individual into sharing sensitive information or to perform inappropriate tasks such as transferring money from one account to another (e.g., through fake text or email to a finance officer).

The foundational basis for social engineering involves skill to take advantage of the trust of a targeted person, and this requires having information about that target. Since AI is so good at collecting and analyzing information to establish context, it should be expected that social engineering, including phishing, will become more difficult to stop.

As with nation-state attacks, social engineering attacks will also demand a strategic plan to ensure proper protection. Boards should monitor their companies' defensive programs and should request to see evidence that these are working. Past methods, such as phish testing, will be useful components but will not be sufficient as the basis for such protection plans.

BOARD OBLIGATIONS

The first obligation that every board member should recognize—and this point should be patently obvious—is that a basic working knowledge and baseline understanding of AI is a requirement for modern board members. I wrote this article with this initial goal in mind.

In addition, however, there are emerging tasks that should become part of the day-to-day board ecosystem. While these tasks will evolve over time, let me point out a few below that I expect to see become important in the coming years. Local business conditions should certainly be used to tailor these general points.

Mergers and Acquisitions Must Include AI as a Factor

If the organization regularly performs mergers and acquisitions (M&A), then it must become a standard component of the evaluation rubric that potential AI disruption be considered. The last thing any organization needs is to make a major investment in a company that will soon be disrupted or even replaced by AI.

The M&A team should be directed by senior leadership, with governance from the board, to ensure that this factor is thoroughly considered, especially for mergers that are sizable with consequence to the firm. Without such careful scrutiny, the possibility of a poorly conceived merger or acquisition seems possible—and potentially disastrous.

Human Decision-Making Will Not Be Replaced by AI

A commonly stated point in the popular media, and one that might have some influence on board member thinking, is the claim that AI will replace human decision-making. This may be true in certain situations where data is perused and processed in a structured manner. Radiologists, for example, might replace certain of their data tasks with AI.

The suggestion, however, that this will occur in the context of board strategy, corporate governance, and organization oversight is not reasonable. Good board governance will make use of technologies such as AI to ensure optimal context for discussion and debate, but robots are not likely to gain a seat at the board any time soon.

Cost Reductions Can be Considerable Using AI

One advantage that AI does bring to most business contexts is the ability to reduce cost. Customer care, help desk support, and other tasks that involve procedural steps will be good targets for such reduction. And boards would be wise to establish oversight where such cases are being considered.

The goal, obviously, should be to balance the needs of the firm for cost optimization with the needs of customers, who will demand high quality interactions, and also the needs of employees to feel safe that their career paths will be preserved—or at least guided toward areas that will complement the use of advanced technologies such as AI.

ACTION PLAN

The best course of action for corporate boards and individual board members may have already begun with perusal of this article. Education will be a key differentiator between boards, and any governance team that takes the time to learn the implications of AI will have a clear advantage.

My advice for an action plan is to over-index on education and training. The steps implied by the comments above should be included in local planning, but each organization is different. In the coming years, board members will have to earn their paychecks by developing effective plans for governance and oversight in this new technological era.

CYBERSECURITY IN THE SPACE DOMAIN: SAFEGUARDING OUR FUTURE

SPACE CENTER HOUSTON

International Space Center Mission Control

DAVID NEUMAN

In the quiet and bustling offices of the International Space Station's control center in Houston, Texas, a tension-filled silence suddenly hung in the air. The screens in front of the control team flickered, shifting from the usual display of telemetry data to an ominous black. Only a single line of text remained: "Access granted. Control transferred."

A thousand kilometers above, the International Space Station (ISS) began slowly veering off its usual orbital track, unbeknownst to the astronauts living and working inside. Meanwhile, thousands of kilometers below, another significant event was taking place.

Simultaneously, the global positioning system (GPS) ground stations, a constellation of 24 satellites traveling 12,000 miles above the Earth to provide positioning data to billions of users around the globe, started reporting unexpected anomalies. This wasn't an isolated error; all 24 satellites were rapidly rendered non-operational. The lifeblood of navigation and timestamping systems worldwide was effectively silenced.

Down on Earth, the impacts of this double-edged attack were almost immediate. Air traffic controllers stared at their screens in bewilderment as the positional data of thousands of planes disappeared.

Ships at sea lost their bearings, and self-driving vehicles on the streets came to a bewildered halt, unable to pinpoint their location. Stock markets experienced extreme turbulence as high-frequency trading systems faltered.

In the backrooms of power grids, engineers watched in horror as synchronization of the grid, which relied on GPS timestamps, started to fail, causing blackouts in cities worldwide. At the same time, billions of smartphone users were suddenly unable to access location-based services, severely disrupting daily life and business operations. The world had been rendered blind and lost in space and time.

> **Contemplating the chaos of a major cyberattack on space technology may be easier than trying to imagine a coordinated response.**

At the ISS control center, the staff desperately tried to regain command of the space station. Their concern was not just for astronaut safety but also for the dozens of crucial scientific experiments onboard, many of which had implications for climate research and future space exploration. As the ISS continued its unintended and risky orbital maneuver, the specter of the uncontrollable descent of the 420,000 kg station towards Earth loomed, with potentially catastrophic consequences for those on board and those in the projected impact zone on Earth.

Suppose this hypothetical scenario had actually happened. What would come next?

Chaos would have erupted in the civilian world and within the corridors of power, both domestic and international. A flurry of activity would have begun within various government agencies in the United States. The Department of Homeland Security would have quickly mobilized to protect and coordinate a response to cyberattacks against terrestrial components of the space systems.

And so it went. As they worked tirelessly to manage the impact on civilian infrastructure, the Federal Bureau of Investigation launched a parallel investigation, seeking to identify the perpetrators of the cybercrime. Simultaneously, the Department of Defense, in coordination with the U.S. Space Force and U.S. Cyber Command, focused on the defense of national space systems. Their immediate goal was to restore control of the International Space Station and the GPS satellites while securing other space-based assets against potential follow-up attacks.

The National Reconnaissance Office, tasked with operating intelligence satellites, was also in high gear, scanning through petabytes of data to ascertain if the attack originated from a foreign power. Meanwhile, the National Aeronautics and Space Administration (NASA) provided technical support, applying its extensive expertise on the ISS to help regain control of the wayward space station.

Despite this flurry of activity, there was a palpable sense of confusion and tension due to overlapping jurisdictions and the need for defined responsibilities. It needed to be made clear who should be taking the lead, causing delays in the response and creating friction between agencies. With its responsibility for commercial spaceflight, the Federal Aviation Administration felt sidelined despite the significant impact on commercial aviation and navigation systems.

Internationally, the response was even more fragmented. Nations dependent on GPS scrambled to mitigate the impacts. Discussions started at the United Nations about the need for an international framework for space cybersecurity. The spacefaring nations, each with its own stake in space assets, urgently convened to discuss a joint response. But the absence of an international body with clear responsibility and authority to respond to space-based cyberattacks added another layer of complexity and delay.

This hypothetical is indeed the stuff of science fiction. And yet, it represents a plausible threat in our increasingly interconnected and space-reliant world. The repercussions such an event could have on society and businesses worldwide, from disrupting air travel and telecommunications to causing catastrophic power failures and affecting financial markets, are alarming.

Our future on Earth and in space is irrevocably tied to our ability to safeguard these crucial systems from cyber threats. Hence, the need for technological solutions and international cooperation, for norms and defined responsibilities in this rapidly growing field. This is not merely about preserving the status quo; it's about securing a future where space continues to be a resource that unites nations, propels economic growth, and catalyzes scientific discovery.

WE ARE INTERTWINED WITH THE SPACE DOMAIN

Our entanglement with these space systems stretches far wider and deeper into our everyday lives and societies than one might initially realize. A look at satellite communications, weather forecasting, climate monitoring, and other dependencies throws this into stark relief.

An attack on satellite communications, the backbone of global connectivity, would go beyond merely obstructing GPS navigation. It would cripple services like TV broadcasts, internet connectivity, and long-distance telephony. This would be particularly detrimental to remote and rural areas, where traditional infrastructure may not reach, potentially isolating entire communities.

Simultaneously, our ability to predict and prepare for severe weather conditions could be dramatically hampered if the satellites that monitor weather patterns and climate trends were compromised. Such an event would not only impair our ability to provide life-saving early warnings for hurricanes or monsoons, it could also compromise our long-term understanding of climate change, with far-reaching implications for the planet.

Similarly, an attack on space-based systems that support precision agriculture, global financial systems, emergency services, and scientific research would prove devastating. Farmers could face massive agricultural losses without the weather data they rely on. Disruptions in the precise timestamping provided by GPS satellites could send shockwaves through global stock exchanges and banking transactions, potentially triggering widespread economic instability. Additionally, we rely on emergency services for safety and security, such as fire, police, and ambulance services, which could significantly increase response times without reliable navigation systems. Finally, pursuing knowledge could be stalled, as researchers across various fields—from wildlife migration to astronomy—rely heavily on satellite technology for data gathering and observation.

THE COMPOSITION OF SPACE SYSTEMS AND OPERATIONS

This extensive network of dependencies highlights the need for robust and proactive measures to safeguard space-based assets from the looming threat of cyberattacks. Protecting space systems requires cyber defenders to fully grasp intricate operations and interconnections. Like an enterprise, these systems contain many connected components, each potentially a vulnerability that adversaries could exploit. Comprehending how they fit together, function, and interact is key. It empowers defenders to anticipate threats, implement protections, and maintain resilience.

Securing assets from cyber threats isn't just about guarding individual components. It's about protecting an entire ecosystem, which demands a holistic understanding of the system's architecture and operations. In the intricate ballet of global communication, space-based assets such as satellites, space telescopes, and space stations perform their dance high above the Earth. Each celestial body houses its onboard systems.

Think of these as the asset's brain—containing computer processors, storage, sensors, and communication antennas. Some even have thrusters for maneuvering. This array of onboard systems receives commands from Earth and manages the assets' daily operations, ensuring the harmony of their orbital dance.

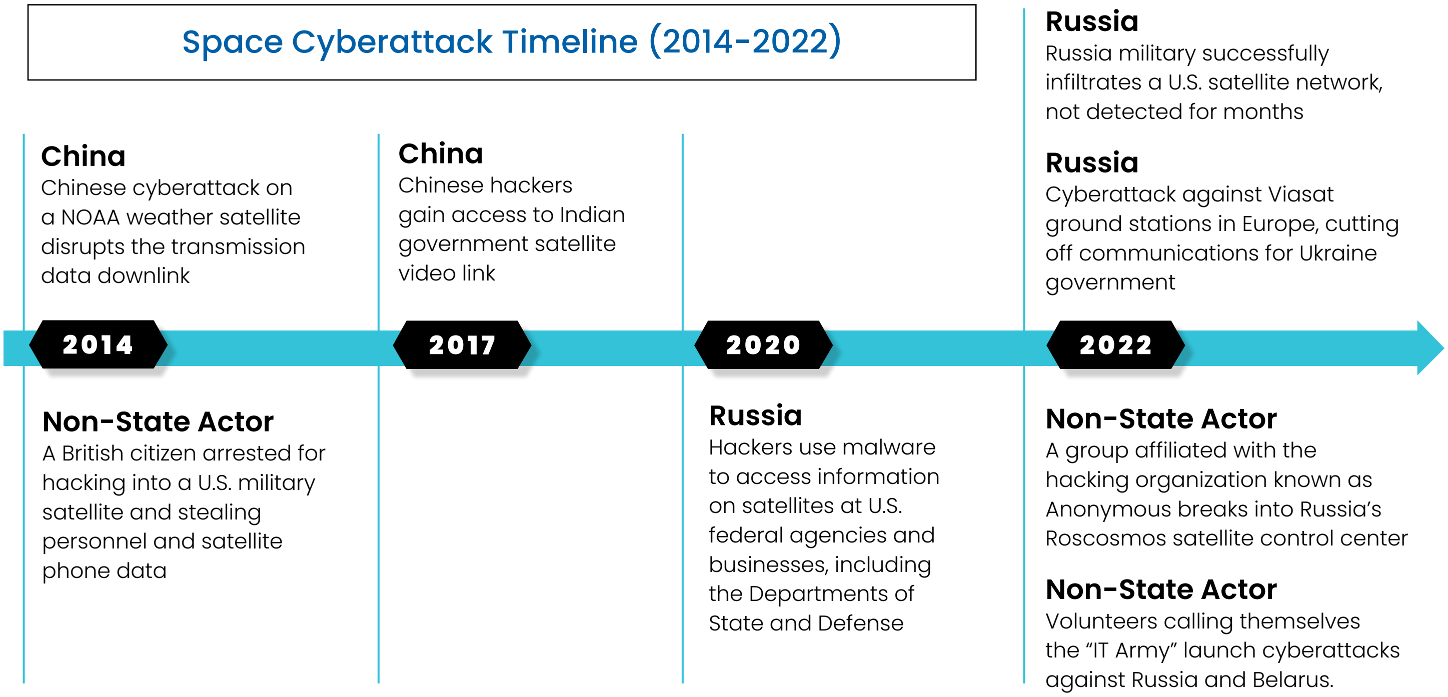
On the Earth's surface, the dance partners of these space assets are the ground stations, each equipped with large antennas. Positioned strategically around the world, they maintain a constant pas de deux with the satellites, undeterred by the Earth's rotation. Here is where the conversation happens—ground stations dispatch commands to the satellites and, in return, receive a cascade of data. They function as the essential terrestrial connection points in this vast space communication network, transmitting and receiving signals like the ebb and flow of an electromagnetic tide.

But the dance does not end there. The data, once received, embarks on a new journey, coursing through terrestrial networks toward data centers scattered across various locations. The frequencies and technologies forming these communication links vary, fine-tuned for the type of satellite and its distance from Earth. The information is processed, stored, and analyzed in these data centers, converting the raw data into a comprehensible format for further use.

Finally, these data centers also take on the pivotal role of a command hub, from which operators send instructions to the space-based assets. This intricate network, stretching from the silent void of space to the bustling data centers on Earth, forms a complicated choreography far more elaborate and interconnected than traditional technology systems. Understanding this network is vital to appreciating the sophistication of our modern space infrastructure, and the vulnerabilities that must be secured to protect it.

THREATS TO SPACE OPERATIONS

While specific details about cyberattacks on space systems are often classified or undisclosed due to national security concerns, several recent incidents shed light on the types and severity of such threats. These real-world attacks illustrate the diversity of the space ecosystem's cyber threats, ranging from service disruption to espionage. The threats can come from various sources, including nation-states, non-nation threat actors, and individual hackers. (I have created below a timeline of recent space-related attacks, including published attributions of the attackers.)



Space Cyberattack Timeline (2014-2022)

2014

China
Chinese cyberattack on a NOAA weather satellite disrupts the transmission data downlink

Non-State Actor
A British citizen arrested for hacking into a U.S. military satellite and stealing personnel and satellite phone data

2017

China
Chinese hackers gain access to Indian government satellite video link

2020

Russia
Hackers use malware to access information on satellites at U.S. federal agencies and businesses, including the Departments of State and Defense

2022

Russia
Russia military successfully infiltrates a U.S. satellite network, not detected for months

Russia
Cyberattack against Viasat ground stations in Europe, cutting off communications for Ukraine government

Non-State Actor
A group affiliated with the hacking organization known as Anonymous breaks into Russia's Roscosmos satellite control center

Non-State Actor
Volunteers calling themselves the "IT Army" launch cyberattacks against Russia and Belarus.

Why is space particularly susceptible to cyber threats? While space assets share similarities with those affecting terrestrial systems, several factors make them uniquely vulnerable. Assets such as satellites are designed to operate for many years, sometimes even decades. This longevity means their onboard security can quickly become outdated, making them more vulnerable to evolving threats. Once a satellite is in orbit, it's virtually impossible to physically access it for repairs or upgrades. Therefore, any security vulnerabilities present at launch, or those that arise due to changing threat landscapes, can't be rectified.

Due to the inherent latency in communication with space assets, and the limited processing capabilities of many satellites, sophisticated real-time intrusion detection and response measures take time to implement. The radio signals used for satellite communication can be relatively easy to intercept, jam, or spoof, especially those of lower-frequency bands, unless protected by strong encryption and authentication measures. Components for space assets often come from a global supply chain, increasing the risk of compromised hardware or software being included in the final product.

Given these challenges, cybersecurity in the space domain requires specialized strategies and solutions that go beyond the measures employed in traditional IT systems. It calls for secure design and manufacturing advances, robust encryption and authentication protocols, secure and reliable command-and-control systems, and international cooperation to establish space-specific cybersecurity norms and practices.

SECURING SPACE AGAINST CYBERATTACKS

As we extend our reach into the cosmos, security becomes paramount. This reality is rendered more pressing as the scope of our space economy continues to expand. The 5,400 satellites currently in orbit will be dwarfed by the anticipated launch of more than 24,500 satellites over the next decade. Commercial ventures will account for over 70% of these new celestial bodies.

The escalating significance of these assets to the global infrastructure, and the mounting sophistication of cyber threats, underline the urgency for innovative solutions. However, the unique hurdles presented necessitate a different approach than we typically employ to tackle traditional cybersecurity issues.

Several solutions are emerging, each addressing the specific cybersecurity demands of the space domain. Quantum encryption, for instance, is leading the way in communication protection between space assets and ground stations, as traditional encryption methods risk obsolescence in the face of advancing quantum computing. AI and machine learning are emerging as invaluable tools for real-time threat identification, sifting through massive data sets to improve response times and system resilience.

As our space assets multiply, secure space traffic management is becoming increasingly vital for identifying potential cyberattacks and ensuring safe operation. A commitment to cyber resilience in space systems design is essential. Building these systems with cybersecurity as a cornerstone from inception will help ensure they can withstand future threats.

In an increasingly interconnected world, establishing international cybersecurity standards for space could unify and enhance the security of all spacefaring nations and companies. And leveraging blockchain technology could help secure the integrity of hardware and software used in space systems, mitigating a significant source of the threats.

Finally, strengthening the security of land-based components, such as ground stations and data centers, is crucial to a holistic space strategy. By integrating these innovative technologies and approaches, we can fortify the cybersecurity of the space domain, securing the critical services we rely on now and will continue to rely on in the future.

THE TAKEAWAY

My hypothetical cyberattack was designed to serve as a sobering reminder of the potential vulnerabilities and profound consequences of such an attack on our space-based systems. I hope it underscored thought-provoking questions about our preparedness, the interconnectedness of our world, and the urgent need for action.

Moreover, the response portrayed in our scenario highlights the challenges of coordinating a timely and effective counter to space-based cyber threats. Overlapping jurisdictions, a lack of defined responsibilities, and the absence of international protocols create confusion and delays, leaving us vulnerable. It emphasizes the critical need for collaboration and clear lines of authority to ensure a swift and coordinated response.

I hope the scenario also underscored the unique nature of space as a domain for cyber threats. The longevity of space assets, the difficulty of access for upgrades, and the global supply chains make them particularly susceptible to evolving risks. We must recognize the distinctive characteristics of space systems and develop tailored strategies to protect them from threats that transcend traditional cybersecurity approaches.

Our future, on Earth and beyond, is inseparable from the space domain. It is time for governments, organizations, and individuals to prioritize the protection of our space-based systems and preserve the benefits they bring. Will we unite to strengthen resilience, foster international collaboration, and establish robust frameworks to defend against space-based cyber threats? The answer will shape the future of our interconnected world and determine whether space remains a beacon of unity, innovation, and exploration.

NASUNI®

Nasuni is a leader in hybrid cloud storage, revolutionizing file data solutions. Their File Data Platform offers unmatched scalability, edge performance, and data security, eliminating traditional NAS limitations. With innovative features like ransomware protection and seamless transitions, Nasuni empowers businesses to scale efficiently, reduce risks, and optimize operational costs.

TAG
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG SECURITY ANNUAL