Cyber Sovereignty: Governance, Risk, and Strategy to Win the Invisible War

By Dr. Nuru-Deen Mohammed, CISM

Nurudeen.mohammed@mail.waldenu.edu

07/07/2025

Abstract

As the world becomes dependent on digital processes, both government and corporations face new threats. Holding data for ransom, stealing or compromising data can now have disastrous consequences, disrupting essential processes.

In the face of these new risks, where the digital world has become the battlefield for security, a new approach must be adopted to identify threats, manage risks and secure data and infrastructure. By adopting a strategic GRC approach that place data security at the heart of operations and allow for private-government initiatives to share threat data, the new digital battlefield can be controlled.

Keywords

Cybersecurity; Governance, Risk and Strategy; Strategic GRC; Data Security; Digital Security.

Introduction

Cybersecurity has been a threat since the very beginning of the digital age, but it has evolved considerably since those early days. Where once a DDoS attack to take down a forum or overload a website was a technical challenge to overcome, today, not only are the attacks more sophisticated, but the targets have changed too.

As businesses and governments alike rely on digital infrastructure for mission-critical processes, daily operations have become ever more at risk from cyber threats. The potential cost of successful attacks in both monetary terms and loss of operations could cripple government activities and bring corporations to a standstill, with all the damage and repercussions that they bring.

The digital space has become the battleground of an invisible war, where governments and corporations alike fight endless attacks designed to suppress, infiltrate, steal, and collapse data, infrastructure, and activities.

The New Battlefield: Cyberspace as the Arena of Modern Warfare

Cyberspace has taken on a new meaning as the battle for supremacy of digital assets and systems has matured. Through digital infrastructure, attackers can hold data for ransom, halting business or government operations until vast sums of money are handed over.

While this has been going on far longer than most of us realize, with the first recorded incident of ransomware taking place in 1989, targeting attendees at the World Health Organization (Wikipedia, n.d.), it was the 2021 attack on the Colonial Pipeline (Cybersecurity

and Infrastructure Security Agency, 2023) that showed just how devastating such an attack could be.

Aimed at the largest fuel pipeline in the US, this ransomware attack caused gas shortages and widespread panic until $4.4 million in payments were made. A hint of how digital threats could and have disrupted the real world in a significant way.

But it's not always about money, the digital arena has become the battlefield for direct attacks on infrastructure of all kinds, with the SolarWinds attack in 2020 highlighting the risks involved for both state and private operations. The target was SolarWinds Orion, designed for monitoring and management of large IT infrastructure installations. Used extensively by government departments and private enterprises alike, the attack added malicious code that allowed the attacker to send administration-level commands to any infected installation.

The result was chaos, with thousands of crucial systems around the world shut down, bringing major corporations to a halt, disrupting government operations, and more. Data was compromised, including strategic government data, with approximately 18,000 separate systems affected globally. A year later, UK and US security agencies announced that SolarWinds was the result of an attack by the Russian Foreign Intelligence Service, SVR (National Cyber Security Centre, 2021).

If governments hadn't been taking the threat of cyber attacks on their infrastructure seriously before, they were after that. Now the battlefield is no longer in the physical world, government agencies have built sophisticated tools for both attack and defense entirely in the digital space.

Defense against any threat is essential for modern international security, and major nations all have dedicated cybersecurity departments within their intelligence agencies. Here, both defensive and offensive tools and strategies are developed. It's not just state actors either, with corporations at significant risk, advanced defense strategies are created and deployed by these organizations, with significant resources dedicated to digital protection.

With incidents like the Colonial Pipeline and SolarWinds showing just how effective cyberattacks can be, it is no surprise that the number of these threats is rapidly increasing, as both state-sponsored organizations and private enterprises look to take advantage. Whether it is a state's infrastructure, or the valuable data held by large corporations, the value of a successful attack has attracted organized crime, rogue states and corrupt businesses looking to harm competitors and extort millions of dollars.

Corporate Fraud and Digital Insider Threats

While Governance, Risk and Compliance (GRC) has adapted to the digital stage, there are flaws. GRC tends to focus on external risks, cyberattacks, ransomware and so on, and this can leave an organization vulnerable in other ways. Internal manipulation of data, such as financial fraud or simply altering crucial data, can lead to devastating consequences and massive losses for organizations, yet it is barely considered in many risk assessments.

This has manifested through several high-profile incidents involving insider manipulation, including the Wirecard Scandal in 2019/20 (McCrum, 2020). Here, around €1.9 billion

disappeared from the company's accounts over about a year, leaving the business insolvent. Although legal proceedings are still ongoing, a number of Wirecard executives, including the CEO, have been formally charged with the fraudulent activity involved.

Another example that was purely about data rather than financial fraud was the 2017 data breach at credit bureau Equifax (Fruhlinger, 2020). Hackers accessed the personal data of over 140 million individuals across the U.S., Canada, and the UK, including social security numbers, dates of birth, addresses and in some cases even driver's license numbers. This was the result of external exploits, but although they discovered the breach in July 2017, the company waited until September 2017 to publicly announce the breach. The result was Equifax spending hundreds of millions in settlements in all three countries, with over $700 million in fines from the U.S. alone (Federal Trade Commission, 2024).

The lesson that every company must take from these and similar incidents is that risks can be both external and internal, and relying on compliance with current legislation for protection simply is not enough. Instead, organizations must be proactive in their mitigation of cyberthreats, implementing systems that detect internal anomalies just as well as they do external ones.

National Security and the Need for Intelligence-Led Cyber Governance

With the digital space the new battlefield, we can see how corporations have been exposed to considerable financial losses as a result, but the same applies at the state level too. Think about any service a government may provide these days, and it all involves digital processes. In some countries, this has been embraced more than in others. In the UK, for instance, Passports, Driver's Licenses, and more are all connected to the same biometric information (UKGovernment, 2025) for identity confirmation, with UK citizens able to apply for any of these entirely online.

The U.S. has not gone as far, but data on citizens is held digitally in all developed countries, and it goes further. Each government relies on digital communications for almost every aspect of daily operations, from financial transactions to interdepartmental communications. Increasingly, data is centralized for efficient use, increasing risks and providing significant targets for potential attacks.

Looking closer at those risks, an incident such as SolarWinds shows how entwined the commercial and government risks are. A commercial attack from government operations around the world, and it is a similar story with the Colonial Pipeline attack. There, an extortion attempt ended up causing major disruption to gas supplies, requiring drastic government intervention for public safety.

How do you define the Colonial Pipeline attack? Is it a criminal case of extortion through ransomware, or is it an act of war against the infrastructure of the country? It's both, and the challenge governments across the world face is dealing with that scenario.

Increasingly, attacks on corporate infrastructure are attacks on state systems, as the two become so intertwined. The result of that is that while intelligence agencies remain primarily concerned with state-level threats, they must also include corporate cybersecurity as part of

that remit, whether from overt state actors such as other intelligence agencies, state-sponsored organizations that offer a level of deniability, or sophisticated criminal gangs.

Strategic GRC: A New Weapon in the Cyberwar

The need to go beyond the GRC we are used to is clear. It lacks the scope to protect against the wide variety of threats, both internal and external, that corporations currently face. However, the foundations for an effective system are in place, with the new approach known as strategic GRC (Sumner, 2025).

By adopting a new model that incorporates continuous monitoring to identify any potential breach as it occurs, organizations can respond as attacks occur, preventing the kind of data theft that Equifax suffered, or blocking the ransomware insertion that cost so much in the Colonial Pipeline attack.

This does require real-time decision making, however, so that appropriate action can be taken in time, but what does all that look like in reality? Zero-trust architecture should be a universal norm, requiring verification for every action. In this kind of framework, every user is always known, every action they perform is verified, and with segmentation, a breach only has access to limited data.

This approach lowers risks considerably, and when combined with real-time monitoring, provides exceptional protection from both internal and external threats. That continuous monitoring also brings additional benefits, providing valuable data on the nature of threats and attempted incursions. Data collected by multiple systems and organizations can be combined for use with threat intelligence systems (Kosinski, 2025), which analyze attacks to refine security provisions and aid in decision making during attacks.

This same data can be used with predictive algorithms to accurately assess risk and identify where and when attacks are most likely to occur in the future. Together, these processes provide exceptional insight into risk management and threat responses, helping to maintain system integrity.

Because they face similar threats, and in some cases threats from the same attackers, those responsible for cybersecurity in major corporations should seek alignment with the strategies and approaches of national cyber defense organizations. By following the National Cyber Strategy and its objectives, from protecting critical infrastructure to monitoring and countering attacks on data, organizations adopt best-practice solutions for cybersecurity at all times.

The reality is that the digital landscape is an area where cooperation between business and government agencies delivers improved security for all, especially in an era of rapidly growing threats.

Winning the Cyberwar: What Governments and CEOs Must Do

What this means for governments and CEOs is significant change. Reliance on GRC as it is understood today leaves both commercial organizations and government infrastructure

vulnerable to attacks of all kinds. These changes begin with policy changes to address these current and emerging threats.

These include:

- **Data Sovereignty Laws –** With more and more systems utilizing cloud-based systems, Data Sovereignty, the idea that data must be governed by the laws where it is held, is increasingly important. How these laws apply to cloud-based operations must be clearly defined so that appropriate protection can be provided.
- **Global Cyber Treaties –** Many states have multiple treaties regarding everything from trade to defense partnerships with other states. It is a common, accepted approach to dealing with threats and risks in the world. This same stance needs to be part of the digital world too, whether it is data sharing for risk assessment and predictive analysis, or the development of new defensive solutions to protect data and infrastructure.
- **Public-Private Intelligence Collaboration –** Unlike almost any other area of security, the threats posed to the state are the same as those facing corporations. Not just the same type of threat, from hacking and ransomware to data theft, but often the same organizations operating those threats. Working with state intelligence agencies, pooling data and analysis allows all parties to improve threat response and refine threat intelligence to identify vulnerabilities and emerging risks quickly and effectively.

Along with these policy changes, organizations need to adopt internal reforms aimed at ensuring improved protection, better responses, and long-term risk reduction. Board-level cybersecurity oversight should be mandatory, emphasizing the importance of the subject, but also avoiding a common issue, a knowledge gap between the board and those delivering security provision.

Scenario-based GRC provision allows organizations to take into account potential threats from any source, internal or external, enhancing security overall, while mandatory cyber drills help identify weaknesses and allow for rapid responses to real threats by removing uncertainties.

The result of these reforms is an organization that has better informed leadership, better prepared systems and improved overall strategies for both identifying and responding to cyberthreats. However, cyberattacks are always evolving; new technology, new ideas, and new vulnerabilities mean that the risks are never fully contained. In the long term, cyber deterrence has to become an integral aspect of all infrastructure from the design stage, baked into systems and processes to provide continual evaluation and threat detection. This kind of digital resilience delivers a framework of protection against known and emerging threats, but protection should go beyond cybersecurity itself. Digital resilience also includes the way an organization uses data, the resources it has available for recovery, and so on. A holistic approach to data and digital security, from use through security and recovery, all play a part.

Conclusion

Digital threats are only increasing in frequency and sophistication, posing existential risks to both government and private organizations at all levels. Taking on these emerging threats

means adopting new and effective solutions for identification, response and neutralization of cyberattacks.

Strategic GRC brings together leadership response, ongoing security improvements and data sharing between targets, whether private or government, to develop effective solutions for any cybersecurity risk as they emerge.

References

Cybersecurity and Infrastructure Security Agency. (2023, May 7). *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*. Retrieved from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Federal Trade Commission. (2024, November). *Equifax Data Breach Settlement*. Retrieved from FTC: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

Fruhlinger, J. (2020, February 12). *Equifax Data Breach FAQ*. Retrieved from CSO: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Kosinski, M. (2025). *What is threat Intelligence*. Retrieved from IBM: https://www.ibm.com/think/topics/threat-intelligence

McCrum, D. (2020, June 25). *Wirecard: The Timeline*. Retrieved from Financial Times: https://www.ft.com/content/284fb1ad-ddc0-45df-a075-0709b36868db

National Cyber Security Centre. (2021, April 15). *UK and US call out Russia for SolarWinds compromise*. Retrieved from National Cyber Security Centre: https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise

Sumner, J. (2025, April 25). *Beyond Compliance*. Retrieved from GRC World Forum: https://www.grcworldforums.com/risk/beyond-compliance-leveraging-integrated-grc-for-strategic-advantage-and-long-term-success/10165.article#:~:text=Leveraging%20GRC%20for%20Strategic%20Advantage,strengthens%20this%20long%2Dterm%20sustainability.

UKGovernment. (2025). *Biometric Information*. Retrieved from Uk.Gov: https://www.gov.uk/government/publications/biometric-information/biometric-information-introduction-accessible

Wikipedia. (n.d.). *AIDS (TrojanHorse)*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)