ArxNimbus

# The 2024 Digital Risk Checklist

## *Essential actions now, to modernize the management of digital risk and avoid adverse losses*

### ☐ Gain Litigation Preparedness

Nearly every major breach, and many smaller ones, have inevitably been followed hours later with the emergence of class-action lawsuits on the part of shareholders primarily, but also other stakeholders. We now have, by 2023, an extensive body of cases and records of court testimony and documentation surrounding the typical trajectory and structure of these cases. What this court data shows, is that there is a common focus on how the defendant organization went about evaluating and formulating the protective technologies, solutions and processes it had put in place, in the execution of its fiduciary obligations to the shareholders' legitimate interests – *before* the incident.

Time and again, testimony, documentation and discovery reveals that the bulk of these decisions examined in the courtroom and chronicled through depositions turn out to have been driven by professional opinion and expert judgement. One can imagine the heightened scrutiny and exposure for the enterprise as a result of this reality. In the medical profession, physicians learned long ago that malpractice claims are exaggerated when a data-driven diagnosis is not present or cannot be properly defended by diagnostic data. In the 1870s, an absence of a scientific, data-driven diagnosis of the patient condition as a predicate for prescribing treatment, was literally outlawed. It's called experimentation, which is no longer legal on human patients. So if it's illegal for human risks, why should it be an acceptable practice on enterprise risks? And are we really ready to accept the costs of litigation exposure that these legacy methods are shown to incur?

Many recent actions on the part of the SEC and others, show an aggressive trend toward not only holding organizations liable (as in the current SEC fraud suit against SolarWinds), but also to name senior management, including the CISO, as individual defendants. Unlike historic

or conventional cases of corporate wrong-doing, cybersecurity liability has no process for assembling a defense based on accepted practices like GAAP (Generally Accepted Accounting Principles). In this environment, as shown by the filings in these cases, the primary set of principles that SEC and others are out to discover adherence to, are those of NIST cybersecurity frameworks including NIST CSF and NIST 800-53.

How will you demonstrate, prove, and establish in a court case, that the organization has in fact adhered to NIST standards? How will you show that your risk exposures were properly assessed and evaluated in terms of NIST? How do you plan to document the way the organization chose certain protections, solutions and strategies based on NIST-centric evaluation? How will you show that the guidance of the cybersecurity budgets and overall program are in adherence to NIST standards?

***Immediate Actions:*** Move past the adverse risk and cost exposure of marginally defendable digital risk programs by getting to a thorough risk profile that informs specific actions and preventive measures traceable and documentable back to accepted regulatory frameworks. Be able to document the economic tradeoffs that were considered in the shareholders' interests – before an incident happens. Build preparedness for any adverse litigation by having a recurring set of understood and recorded linkages between the best-available projections of cyber risk and the resulting actions taken to mitigate those effects. Don't go without this preparedness – get ahead of the massive associated costs now – before a situation develops.

## Reduce Geopolitical Threat Exposure

Increasingly, Nation-State threats are a real and expanding source of risk. These weaponized attacks are in an entirely different class – with entirely different aims – than the conventional threats of the past. With several major global conflicts ongoing, combatants will attack wherever they can punish their adversaries – even simply for publicity or intimidation. Many conventional security programs assumed these to be rare if not infinitesimal probabilities – this is no longer reality. Infrastructure, Financial Services, Defense, and other industries are all at risk to the rapid escalation of global geopolitical factors.

***Immediate Actions:*** Acquire and implement real-world risk solutions that include the full scope of exposure, including Nation-State threats. Implement threat metrics and assessments that conform to recognized threat taxonomies like MITRE ATT&CK®. Do not accept the velocity of attacks in your industry and other emerging indicators to be omitted from your analysis and understanding. Properly measure your exposure and probabilities around these potentially catastrophic risks, based on current, objective risk data. Work with key advisors who have real-world, first-hand experience in combating global Nation-State attacks.

ArxNimbus

## Evaluate and Erode SBOM Exposure

The rapid expansion of risk exposure through the "internal" compromise of application software and utilities is alarming. The majority of these issues, including well-publicized losses associated with commercial software like Kaseya, SolarWinds, MoveIt and others, have been found to originate with the use of open-source code, or portions of code, that itself contains certain malware. This malware then ends up being distributed to all users via upgrades and installations on the part of unsuspecting customer organizations.

How can you avoid and/or eliminate this rapidly growing source of risk exposure and loss? Increasingly, the answer lies in properly understanding the lineage or heritage of the software applications one is running and/or evaluating and selecting. Through work done by Allan Friedman and others in organizations like CISA, the ability to establish a "Software Bill of Materials" (SBOM) is coming into use. An SBOM, as the name implies, is essentially the family tree depicting the origins of the code that currently comprises the application being run. This allows users to determine the degree of open-source software (i.e. code originating from un-vetted sources) that may be embedded in each application. The more open-source code, the higher the potential for exposure

***Immediate Actions:*** Establish SBOM as a key evaluation requirement for all new software applications before purchase, licensing and implementation. Work with corporate procurement to make this an enterprise-wide requirement to be applied to any software purchases, whether within the domain of IT or not, including Operations, Manufacturing, Marketing, HR, and other key departments. Organize an ongoing effort to evaluate pre-existing software and determine an SBOM for each application. Contact vendors and make them aware of the organization's SBOM requirements and establish a date for compliance on the part of each vendor. Build and maintain a library of SBOM documentation, including a master catalog of all software applications, and which have met the requirement for SBOM reporting, and which applications have satisfied company criteria as to the level and exposure of open-source code. Incorporate open-source exposure into overall risk management assessments and analysis to properly reflect this significant and growing source of risk exposure.

## Use Data to Accomplish Compliance

There is an escalating level of skepticism among regulators regarding organizations' self-reporting of their risk status. This skepticism is exemplified by recent SEC rulings, such as those mandating a data-driven evaluation of digital risks

(https://www.sec.gov/rules/interp/2018/33-10459.pdf). Regulators and auditors are increasingly reluctant to rely on unverifiable assessments and expert judgment for compliance sign-off.

***Immediate Actions:*** To navigate this changing landscape, it is essential to establish processes that meticulously trace digital security initiatives, priorities, and funding (e.g., compliance efforts) back to regulator-mandated requirements and frameworks. Develop comprehensive support documentation that enables the presentation of results to regulators and during compliance review meetings in a manner recognized and understood by state, federal, and industry reviewers, adhering to standards like FFIEC, NIST, FERC, ISO, and other relevant benchmarks. Ensure readiness to connect actions, projects, and achievements to specific detailed requirements originating from relevant sections of regulator-driven frameworks. In essence, being well-prepared with proper documentation significantly enhances the likelihood of receiving due credit for compliance efforts.

## ☐ Address IoT Exposure

The rapid proliferation of IoT ("Internet of Things") devices is a notable trend, with projections estimating an increase to 60 billion devices by 2026. The IoT landscape represents an expanding "threat surface," characterized by its vulnerability and emergence. A recent Forbes analysis emphasizes the need for proactive measures, stating that developers and service providers in the IoT and industrial IoT (IIoT or "ICS") realms should embrace new privacy laws and cybersecurity measures. The analysis underscores that security considerations must be integral from the outset, advocating for a strategic approach and collaboration with tech ecosystem partners to bring the most secure devices, applications, clouds, systems, and connectivity to the market, thereby expediting success.

***Immediate Actions:*** In response to the growing IoT landscape, it is crucial to incorporate IoT exposure into all digital risk analysis and risk management models. This entails a comprehensive assessment that properly weighs the IoT-related risks against the broader context of enterprise-wide risk. The goal is to accurately quantify the potential loss exposure and ongoing costs associated with these risks, often referred to as the "self-insurance cost." By doing so, organizations can proactively manage and address the risks stemming from IoT, promoting a more resilient and secure operational environment.

ArxNimbus

## Risk-Manage your Entire Cloud Landscape

Migrations to the cloud, operations in the cloud, application of hybrid cloud architectures – all of these dynamics represent significant sources of risk exposure. Is there sufficient visibility into these risks – not from merely qualitative impressions but rather fact-based – before, during and after each of the various applications and migrations associated with cloud deployment? The cloud economy is large and expanding. The economics warrant cloud strategies and architectures being a core part of every organization's technology strategy. But it takes proper management of the way that cloud migrations result in fluctuations – near and mid-term – in the risk profile and associated costs affecting the enterprise.

***Immediate Actions:*** As with other dimensions of risk affecting the enterprise, make certain that leadership is in possession of a cloud-aware, data-driven analysis of the functional and economic consequences of risk. This includes analysis that is consumable and relevant for Internal Audit, the CFO, CIO, In-house Counsel, Risk Management, and of course the CISO and cybersecurity organization. Getting a cloud-sensitive profile of risk that allows these key stakeholders a common view and understandable metrics allows for reasoned and properly weighted choices to be made in the strategy and tactics of cloud-enabling security to be made from a basis of real trade-offs.

## Properly Guide Insurance Decisions

Increasingly, commercial insurers are providing attractive and materially useful policies allowing the transfer of digital risks – cybersecurity risks – away from the enterprise. But how do we know how much to address through these policies? In a recent case, a major breach resulted in $1.4bn in losses while the company had just $40mm in cyber insurance in place. How were they estimating their use of cyber insurance? What tools or techniques were they relying on to give them a proper picture of their digital risk exposure – in economic terms?

***Immediate Actions:*** Now is the time to gain a complete understanding of enterprise cyber risk – this provides the only real basis for making informed decisions about how to utilize commercially-available insurance programs to transfer the right level of costs associated with these risks. This all starts with a data-driven analysis of the complete set of risk – and its ongoing cost – that the enterprise incurs as a result of its industry, size, and operations. Only then can we look at the portion of that risk that has already been mitigated through risk-reducing technology and processes. Then and only then can we quantify the remaining or residual risk left to be either mitigated or insured. Finally, risks that cannot be either mitigated or insured represent remaining risk, and these carrying costs must be funded essentially through "self-insurance" in the form of reserves, in order to avoid incurring unfunded liabilities. Needless to

say, understanding these numbers and the relative impact of each of these categories, turns out to be essential to actively managing the overall digital risk landscape.

## Establish 2024-ready, insurance-grade Risk Management

Cybersecurity risk is critically important for all organizations because it directly affects their ability to protect sensitive information, maintain trust, comply with regulations, ensure business continuity, and safeguard their overall financial health and reputation. Proactive cybersecurity measures are essential to mitigate these risks and safeguard the interests of the organization and its stakeholders.

Just like medical tests that are essential to establish a correct diagnosis, comprehensive management of cyber risk is essential to allow correct and targeted efforts to protect sensitive data; maintain customer trust; gain legal/regulatory compliance; preserve business continuity and resilience; secure intellectual property and supply chains, and calibrate correct levels of cyber insurance coverage.

All this while regulators, auditors, Boards and litigants increasingly expect companies to demonstrate the data supporting their decisions and choices in their cybersecurity programs. Risk Management allows for an effective and efficient set of priorities, budgets, solution choices and sustainable security processes.

***Immediate Actions:*** Implement a Risk Management platform that utilizes correct actuarial science models proven in trillions of dollars of insurance coverage and risk assessment. Move past outdated risk models and risk management practices from the 20th Century like Value at Risk ("VaR" or "FAIR"). Establish a backtested, proven data-driven platform for analysis, valuation and alternative-selection on the full scope of digital risk across the enterprise, and the evaluation of the available options to address it.

ArxNimbus

– – –

## About Arx Nimbus

*Arx Nimbus was founded in 2016 to bring quantitative risk management to cybersecurity and digital risk exposure for every organization. Developed under the sponsorship of US Strategic Command, Arx Nimbus' patented Thrivaca Risk Profile profile provides the only financial rendering of the complete risk landscape approved by NIST. Arx Nimbus enables organizations to advance their existing Risk Management efforts, gaining cost recovery, reducing unfunded liabilities and litigation exposure, prioritizing cybersecurity spending and enhancing compliance acceptance.*

# What's Guiding *Your* Digital Risk Program?