CMS
IT SERVICES
Reliable I Robust I Secure

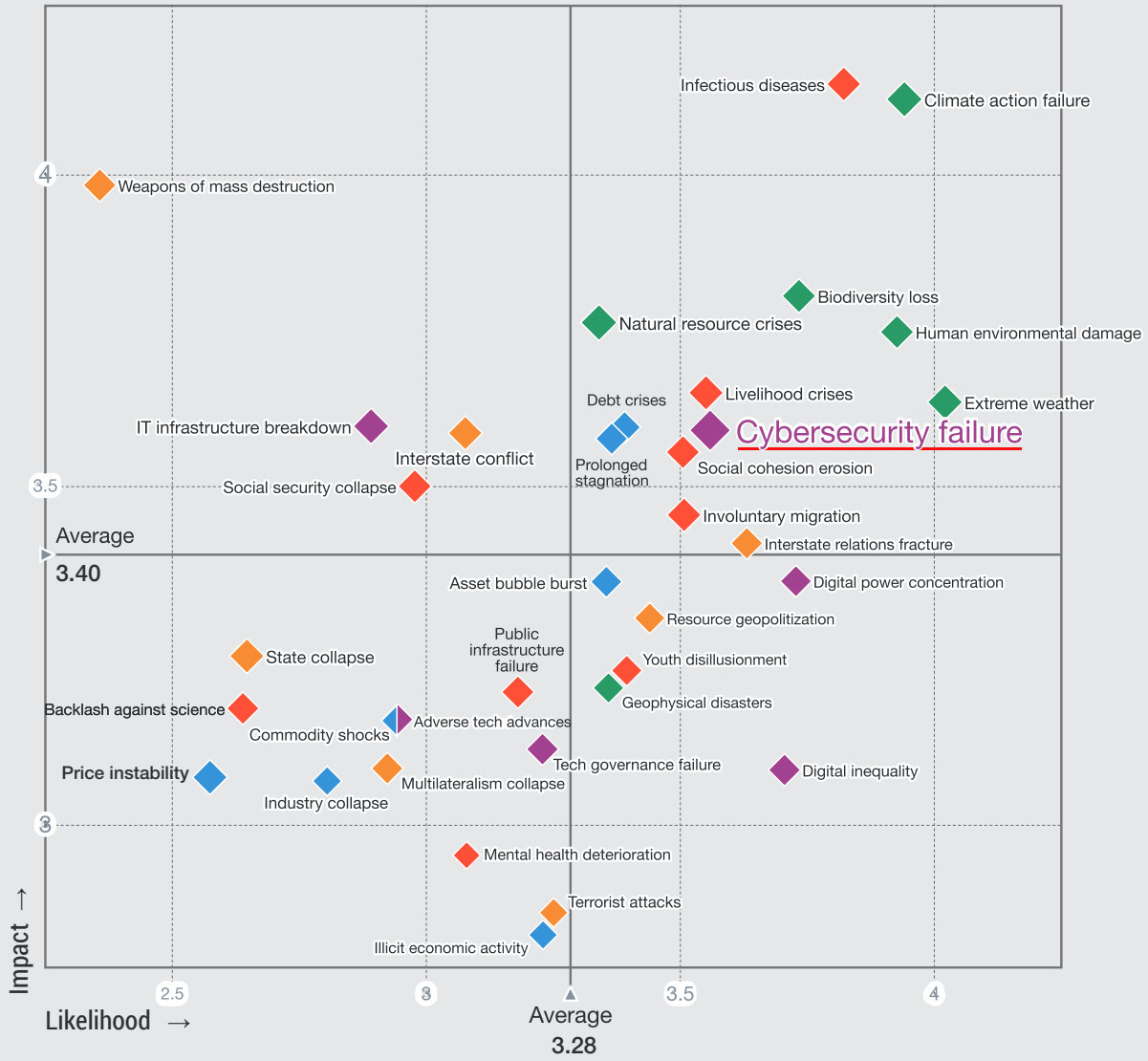
Follow the 5 A's of Identity and Access Management to perk up Enterprise Security

All enterprises, before and since the information age, have data that is essentially and definitively theirs and that is the substance of their business. However, a business of the 21st century has as its business far more than its own business—which is to say, while digitization has taken a business's core data to nerve centers such as data centers, disaster recovery centers, near-sites, and/or cloud, that isn't all that matters for a business today. The channels through which data moves through an organization and beyond it, connecting people, processes, culture, intelligence and technology, are as crucial for enterprises.

As enterprises have evolved to make these connections in digital forms, their networks have become correspondingly complex and multi-layered. The various nodes across which data moves have sundry roles and privileges, and they fulfil them with data harnessed across a web of servers, storage, databases, applications and systems. Keeping an enterprise secure by managing who can do what amid these flows is thus a crucial but complicated task, requiring Identity and Access Management (IAM).

Global Risks Landscape

How do respondents perceive the impact → and likelihood → of global risks?



Cybersecurity Failure was reported as one of the Top 10 Risks overall

Source: The Global Risks Report 2021, 16th Edition, Word Economic Forum

Identity and Access Management (IAM), like the problems it tries to solve, involves many moving components that need to be brought together into a holistic flow. A way to understand and formalize the process would make its implementation easier and ensure that the benefits it brings are indeed manifested in an enterprise.

To this end, consider the 5A framework. Thinking of IAM as a 5A methodology presents it as offering a comprehensive suite of solutions for the whole expanse of areas and entities that are the business of a contemporary business. To ensure that the layers and dimensions of functions that are fulfilled in an enterprise by different people and at different places all come together in a reliable and secure way, the 5A IAM methodology builds on the four building principles of Ikigai:

A1.	A2.	A3.	A4.	A5.
Providing client **assurance**	Integrating comprehensive **authentication** solutions	Improving **administration** continually, without pause	Enhancing client experience through **automation**	Doing all of the above through **analytics**

A1. Assurance:

Enterprise security should have assurance based on Zero Trust (ZTX) principles, ensuring that the intended features, functionality, practices, procedures, and architecture of the Identity and Access Management (IAM) solution are correct, resilient and always functional. The goal should be to keep up with an organization's policies and procedures, controls under constraints, and roles-based access by leveraging robust analytics and administration to conduct identity stores' normalization. This is the process of reorganizing identities from multiple identity stores into one centralized identity store to prevent redundancies, and map and segregate the services and duties associated with each identity. It isn't enough to have an identity and access management system if one can't be sure that it will work in all facets of one's organization, and which is why framing an enterprise's IAM operation with a discrete assurance service is vital.

A2. Authentication:

Enterprises today operate through networks that involve users and devices accessing data in the information ecosystem and linking up with different elements in the network to use that data. The complexity of such operations mandates solid authentication systems to allow access for various processes and services, with robust SSO mechanisms and cutting-edge protocols (such as SAML, OIDC, RADIUS and LDAP), which allow for checking the credentials of associated parties and verifying their digital identities. Associated with authentication, it would be all the more a bonus if the Identity and Access Management (IAM) solution can help clients with related cybersecurity technologies, along with providing ready-made integration workflows. These can all come together to make sure that the various parties and players using a network all work in concert and play fair. Today's enterprises need security that is inherent to its network, rather than something inserted ad hoc afterward, which only robust authentication techniques can provide.

A3. Administration:

It is not enough to merely authenticate users. An Identity and Access Management (IAM) system must integrate that with ensuring the physical security of clients' managed sites, thereby preventing damage to assets, nullifying data exfiltration and preventing the interruption of IT services. This is done through reliable logical identity governance, which involves continually provisioning and deprovisioning users (user lifecycle administration), building automation and self-help methods in password management, policy management, and creation of related workflows and defined approvals. In other words, a comprehensive IAM solution includes administration that provides these services. An Identity and Access Management (IAM) solution's job isn't done when the IAM system is set up. It should stay to evolve as an enterprise changes, helping organizations deal with problems such as fragmented identities—when multiple, redundant digital identities or overlapping data pile up over time—joiners, movers and leavers—i.e. the logistics of managing identities and accounts as users enter a network, shift place in it or leave it—as well as many other use cases. If that is done, IAM is critical in making sure that the enterprise doesn't just change, but also grows.

A4. Automation:

Many processes in managing identity and access involve tasks that are repetitive, which can be automated. This can be achieved with a native Identity and Access Management (IAM) system with automation playbooks that cover a variety of use-cases, as well as third-party automation workflows covering even more tasks. Using techniques such as Robotic Process Automation (RPA) and PICERL methodologies and more, incorporating automation into an IAM solution can help free up labour and time for tasks that need human ingenuity.

A5. Analytics:

The above functions are best enabled and aided with the intelligence of analytics that process an immense amount and range of data on user and endpoint behaviour, network analytics, business applications, identity and access, external anomaly and internal fraud detection, and policy compliance. With that, it is possible for an Identity and Access Management (IAM) solution to be attuned to protect, detect and respond. Through predictive analytics and machine learning faculties, patterns of usage and data flow that are indicative of threats and other problems are swiftly detected, and based on the kind of incident, certain pathways of responses can also be immediately deployed and put into action. Overall, the client's network of users and data stays secure, and value-creation continues unimpeded.

An enterprise's vision determines its cybersecurity needs, which are fulfilled by an IAM solution which gives comprehensive agency over all channels and zones through which data moves. This is a dynamic solution to provide, which is why it is useful to break it down into aspects that can be meaningfully articulated for the specific context of a given enterprise—from assurance based on zero-trust principles to authentication using Aadhaar/Social Security Number-based authentication and MLA (Multi Level Authentication) methods to regular assessment audits administering the management after it is set in place, to robust program operations and governance through automation. If brought together, the 5A methodology adds up to something far greater than the sum of its parts, and IAM yields what it takes for a business to take care of all its business.

CMS IT Services

Venkatadri, 2nd Floor,8, 8A Garvebhavi Palya, Hosur Main Road,
Bengaluru 560068

+91 80 4550 0300
inquiry@cmsitservices.com
cybersecurity@cmsitservices.com
www.cmsitservices.com