IT modernisation in the energy sector: Preventing cyberthreats to critical infrastructure

Received (in revised form): 7th October, 2019

Pamela K. Isom
Deputy Chief Information Officer, United States Department of Energy

Pamela Isom is deputy chief information officer (DCIO) for architecture, engineering, technology and innovation at the United States Department of Energy (DOE). She directs digital transformation and IT modernisation, implementing innovative, safe and mission-focused products and integration services. Leveraging her strong track record of innovation, collaboration, leadership, foresight, and blending mission with IT capability, Pamela is responsible for and maintains exemplary cyber security and data stewardship and is an excellent adviser to senior executives and officials. Before joining DOE she directed application engineering and development at the United States Patent and Trademark Office (USPTO) where she was responsible for innovative, safe and secure solutions that protect intellectual property and associated rights. She brings over 20 years' private sector expertise, working with various clients in financial services, distribution, insurance and public sectors, to the federal government and her achievements have led to numerous recognitions, including being honoured as a GEARS in Government agency awardee, National Inventors Hall of Fame (NIHF) Women of Innovation exhibitor and honours as a trailblazing woman in labour and business. Pamela is the author of a book and numerous publications on various subjects and she has been granted five patents. She holds a Master's degree in information systems management from Walden University and a Bachelor's degree in business administration from Chaminade University of Honolulu.

Architecture Engineering Technology and Innovation, Office of the Chief Information Officer, US Department of Energy, USA
Tel: +1 202-586-5000; E-mail: pkisom@icloud.com

Abstract IT modernisation is essential for safeguarding information and nations are investing in cyber security advancements that strengthen protection of critical infrastructure, including power grids. Renewable energies are incorporated and distribution channels are optimised to adequately supply buildings, homes, vehicles and customer demands, and advancement in energy storage is progressing to accommodate a variety of sources. The Internet, the varying Internet of Things (IoT) and operational technologies (OT) leveraged to meet supply and demand are compelling to customers, yet such capability broadens the risk of vulnerabilities affecting customer confidence. The energy sector is embracing modernisation as a vehicle for mitigating risks through grid modernisation.[1] Energy is an enterprise strategic asset and there remain opportunities for smarter management and modelling so that the state of utilities is known at any given time and energy is continuously available. With analogies to random incidents, scenarios and data as a strategic asset, this paper shares IT modernisation considerations for cyber risk mitigation in the energy sector.

KEYWORDS: cyber security, IT modernisation, energy, smarter data modelling, smarter data management, architecture, enterprise strategic asset, modern enterprise architecture (EA)

INTRODUCTION

Energy is crucial for national security and modernisation of critical infrastructure including power grids is a necessity. That said, organisations are progressing forward with the use and convergence of

operational technologies including advanced metering infrastructure (AMI), various information communication technologies (ICT), industrial control systems (ICS) and supervisory control and data acquisition (SCADA) applications to better manage supply and demand of energy resources from local and remote locations. In parallel, organisations and grids are becoming greater prey to cyberattacks. The infusion of the Internet and operational technologies introduce vulnerabilities and orchestrated, advanced persistent threat (APT) attacks have become more prevalent. These vulnerabilities are due in part to large, complex power infrastructures and networks. The Stuxnet[2] computer worm, for instance, targeted SCADA systems, causing severe damage to equipment run by those systems while presenting normal health indicators to system monitors. The malicious software ran undetected for extended periods of time, cascading and proliferating damages. Vulnerabilities continue because of increased technical debt and non-compliance that are due in part to the need to keep system upgrades current. Breaches can result in massive power supply disruptions, home and building damage, financial instability, health-related illnesses and more.

A CASE FOR IT MODERNISATION

An analogy to influence risk management in the energy sector:

> 'On 13th July, 2019, New York City experienced a blackout impacting customers for a period of five hours, according to the utility service provider (USP). The USP posted in its media relations site that 'a significant electrical transmission disturbance occurred at 6:47 p.m., impacting multiple circuits in the area, and leading to the loss of service to approximately 72,000 customers. We restored power to all affected areas shortly before midnight.'[3]

This example is a reminder that well-architected, modern solutions must encompass continuous, automated detection so that when incidents arise, impacts are minimised. This is due to rapid identification, isolation or quarantine of affected components and self-healing including integrated redundancy, failover and/or alternate channels to sustain continuous delivery and to recover expediently from outages. Retrospection of the NYC incident presents an opportunity for greater risk management through quality assurance (QA) in the age of continuous interconnectivity. QA principles are:

- Holistic, end-to-end monitoring of conditions and outcomes.
  - Monitoring capability entails instrumentation — models, views, and detection — with real-time situational awareness and integrated what if analysis across the entire energy pipeline. Example success measures encompass value-based trigger execution when monitored conditions arise (eg notifications, alerts, systemic responses); and integration of ever changing and never static monitoring in order to minimise the threat landscape;
- Relationship mapping of assets, components and networks.
  - The greater the dependency the greater the impacts in positive and adverse activity. In its simplest form and for the purpose of this article, assets are valuable people, objects and qualities. To be effective an inventory of assets in use and expired must be examined continuously as well as how they are used relative to intent, and by whom. Assets must be known, managed and proper archival and disposal is not an option. The same concepts apply to components; however, components may or may not be an asset. Interdependencies must be understood and validated in order to understand the

reach of transmissions, vulnerabilities, and to isolate breaches. Stewardship is a key factor of relationship mapping and this responsibility if applied properly attributes to rapid anomaly detection within the network. In the NYC example, for instance, rapid detection of the electrical transmission disturbance occurs so that the energy asset is able to achieve its purpose — get power to customers while components are leveraged to complete root cause analysis;

- Recognition of injection and insertion opportunity.
  - Analysis of behaviour and content is key to recognising normal and abnormal insertions. Adequate sensors, meters and appropriate controls can, for instance, inspect and measure the effectiveness of injections in transit and planned. In relationship to the NYC incident, substation bypass is an example automated and potential human injection that could occur in the event of equipment performance deviations.
  - Injection management examines the source and target, determines feasibility status, and either allows, disrupts through redirection and/or destruction or initiates recovery.

Source	What / Where / Who
Feasibility	Examination of the root cause considering environmental circumstances (current, future and historical).
State	Happened, anticipated, needs to occur.
Acceptability	Determines the extent of the insertion and either allows, disrupts and/or initiates recovery.

ENERGY IS AN ENTERPRISE STRATEGIC ASSET

Organisations can contain cyberthreats in the energy sector by treating energy as an enterprise strategic asset. Suggested practices are:

- Application of zero trust;
- Smarter data modelling and management;
- Architecture — the foundation for sustained decision making, evidence-based policies and governance.

Application of zero trust

Today is the era of evolved digital trust or zero trust networking (ZTN) that calculates and establishes trust between entities on demand based on context (situational awareness, location, identity, credentials, policy, etc.) and organisational risk tolerance. As with software defined networks, ZTN evolves around micro-segmentation, creating logical-access boundaries in the form of segments (eg local solar energy conversion and storage). In a ZTN, segments are hidden from discovery, and access is restricted to entitled resources. It should be noted that entitlements are not permanent, but rather exist for a specified duration based on context. In practicality, application of ZTN minimises the risk of a bad actor from gaining access to supervisory controlled devices that substation operators monitor and manage (local and/or remotely) all the while; should such an instance arise, impacts are minimised.

As depicted in Figure 1, intermediary assets verify eligibility before allowing access and continuously manages — adding and removing segments as required. This approach reduces attack surface areas, as more granular protections are established within organisational boundaries and breaches are contained. In the example shown in Figure 1, intermediary trust was established with the policy and context segment prior to initiation of any other requests.

According to Gartner:[4]

- By 2022, 80 per cent of new digital business applications opened up to

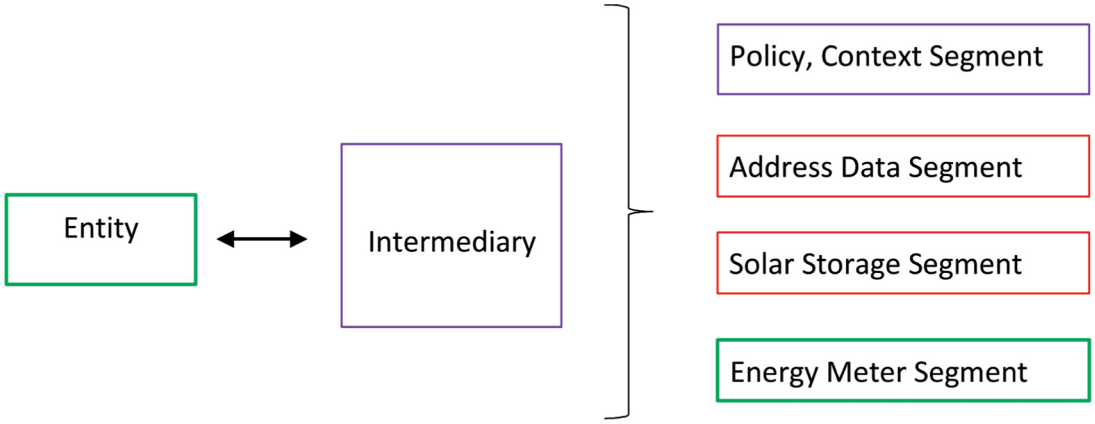

Figure 1: Zero trust modelling is based on segmentation providing greater isolation and containment of breaches. In this example the intermediary trusts an energy service provider entity and therefore grants monitoring rights to the energy meter segment only based on policy and context. Per enterprise architecture and cyber policies, entitlements are for a duration of time, therefore rights do not linger and access requests must be reauthenticated based on context
Source: Author

ecosystem partners will be accessed through zero trust network access (ZTNA);
- By 2023, 60 per cent of enterprises will phase out most of their remote access virtual private networks (VPNs) in favour of ZTNA. Accordingly, perimeters will actually increase in number, becoming more granular and shifting closer to the logical entities they protect — the identities of users, devices, applications, data and workloads.

In summary, application of zero trust mitigates risks in the energy sector greater protecting assets by:

- Adopting a least privilege model that calculates and establishes trust based on context. This approach controls access and reduces the impacts and pervasiveness of attacks because it segments/contains user access to only what is needed;
- Requiring reauthentication each time a user attempts to access data, applications and cloud solutions;
- Persisting continuous logging and inspections for deriving identification, quality analytics and reliable establishment of trust;
- Combining cyber security and risk management practices to immediately identify and assess threats; establish trusted relationships and apply enterprise architecture and cyber policies to assess, respond and remediate.

SMARTER DATA MODELLING AND MANAGEMENT

The North American Energy Resilience Model (NAERM)[5] expresses concerns and provides solutions to approach the breadth and severity of threats against the power grid. The authors clearly state that 'while we must address known threats including extreme weather and cyber, it is equally critical to focus on the next (unknown) threats by anticipating where our adversaries are directing their efforts'.

Considering energy is an enterprise strategic asset means protecting it from bad actors while concurrently examining opportunities to better utilise, maximising availability and minimising the risk of disruptions to customers. This is of particular importance considering the national dependency and diverse energy needs. The DoE maintains collaboration with utility providers, industry, academia and energy

sector organisations to modernise aging grid infrastructures through enhanced communications, the use of modern technology and greater controls. Smarter modelling and management delivers power when and where needed, through the proper channels and at the appropriate times. The backbone behind evolving the infrastructure and grid capability is smarter data modelling and management.

Key characteristics of smarter data modelling:

- Applies scenario-based simulating with situational awareness, integrates cyber risk assessments and is capable of execution with real time data sets and streams. A driver in route, for instance, has no time to wait for a batch process to complete before receiving an electronic alert to brake or for auto pilot sensors to activate in order to prevent an automobile accident. Concurrently, cyberthreat detection should initiate immediately and respond appropriately as per policy;
- Leverages industry, academia and cross-organisational diverse teams of data scientists, subject matter experts, analysts, novice learners and data integrators to generate unbiased data sets and acknowledges subconscious frames of references.[6] Smarter modelling involves not limiting your algorithms to current or perceived conditions;
- Applies security analytics with monitoring to detect threats to the network and possible infiltrations;
- Embeds and prescribes location services, enabling operators, for instance, to dispatch emergency crews for pickup of stranded citizens during natural disasters and knowledge so as to detect whether location data has been tampered with and therefore not trustworthy. It is for this reason that geospatial data must be leveraged for smarter modelling;
- Artificial intelligence (AI), advanced analytics and emerging technologies are not only users of data but can and must be leveraged as tools to validate algorithms, data sets, operating as a testbed for maximising productivity and organisational efficiencies. Adequate models are able, for instance, to legitimately detect and safely and securely redirect battery-stored energy from a homeowner's supply to the community to support demand fluctuations while the homeowner is away on holiday with no adverse consequences to stakeholders or the environment.

Key characteristics of smarter data management:

- Customer and citizen experiences are value advocates. It is therefore imperative to understand the customer landscape and use this data as parameters for models. For instance, in 2014 more than 6m miles of distribution lines and more than 200,000 distribution circuits provided the critical link between the bulk power grid and 160m electricity customers[7] across the US. Generators of electrical power, energy network operators, energy service providers, power retailers, marketers and neighbourhoods are example stakeholders in the energy landscape. Customer experiences and stakeholder data can be used to address questions such as:
  - What are the impacts on legacy users during the introduction of cloud based operational technologies?
  - What steps are necessary to build customer confidence?
  - What choices should be considered to maximise modern, distributed electricity economies of scale?;
- Built-on ontology — energy, security and safety ontology are applied so that data is consistently represented and interpreted by humans and machines. Ontology is domain-focused (eg Smart Grid) and used to describe an area of knowledge and

relationships. Ontology is dynamic and based on context using taxonomies. To mitigate risks, identify metadata for the power network, including system refresh frequency, maintenance, physical and cyber security, and standards;
- Data catalogues are users of ontology. Data catalogues provide a menu of resources, tools, technology and options for users to choose from for data strategy and operational activity including modelling;
- Quality data requires infused data management practices. Oftentimes stakeholders want to but are unable to make data quality improvements due to the complexity associated with change; however, data quality and adherence to data management principles including clean-up must be integrated in data strategy and operations. If an organisation does not have a complete grasp of vulnerabilities to possible cyberthreats, then it cannot effectively protect and defend against those threats. Smarter data management encompasses continuous valuation;
- A talent management pipeline in cyber and data analytics must be continuous in order to keep and exceed the pace of cyber criminals. Scenario planning, penetration testing and cyber security exercises are indicators of a strong talent management programme;
- Ten key performance measures include but are not limited to:
  - Mean time to detect and respond to incidents,
  - Data velocity to and from power stations in normal conditions,
  - Per cent of cyber incidents (including attempts) at the grid and the edge,
  - Per cent of diminished returns due to breaches,
  - Attack campaign indicators,
  - Super user authorisation and access tracking,
  - Critical asset usage, by whom and energy threat ratios relative to dark data,
  - Per cent of service provider (this includes cloud service provider) breaches, recovery services and performance,
  - Per cent of legacy applications in an energy network and known vulnerabilities,
  - System upgrades performed, on target and laggards;
- Common consistent view of data:
  - Considering the 21st-century diversified power needs, the increase in cyberthreats, the bidirectional flow of energy with renewable integration from varying sources (eg wind, solar, micro grids), and complex grid infrastructure that currently is comprised of tightly coupled systems and data, organisations must leverage and maintain an enterprise data referential model (EDRM). EDRM is a necessity for effective data management and governance. It is the instrumentation of organised digital data by subject area rather than by application or other technical delineations. Energy-focused EDRM with business models and scenarios is inevitable as it will be referenced by Chief Data Officers (CDOs), Chief Information Security Officers (CISOs), Chief Innovation Officers (CIOs) and other essential stakeholders to strategically manage customer experiences, and for data collaboration and cyber maturity efforts. Utility organisations will reference EDRM as a mechanism for applying energy management and governance consistency for stronger performance forecasting, planning and outcomes. The ten elements of a strong EDRM can be used interchangeably across people, process and technology to manage energy as an enterprise strategic asset:

1. Governance	Governance is establishing decision rights with mission intelligence so that decisions and policy making are evidence based and sustainable. This must be established and frequently evolve as energy stakeholders and business models evolve. Access rights, for instance, of grid operators occur on an as needed bases applying zero trust principles. Governance formalises ethical decision-making rights with embedded escalations and exceptions that are strategically aligned for continuous protection of assets. Safeguarding information while making data available are at the core of digital ethics. Each of the following EDRM elements require governance.
2. Data discovery and sourcing	What data is used and where is driven by organisational requirements that must be in tune with supply and demand. The quality and reliability of data needs to be evaluated and a plan for use over time put into practice. Determination and validation of distributed energy resources (DERs) are inputs to this element. The use case and scenarios for rapid response to fraudulent billing for utilities, for example, and counter attack measures depend on data discovery and sourcing insights.
3. Data ingestion	This process involves establishment of an ingestion strategy for loading data into an environment. The strategy is typically iterative and based on criteria such as data categorisation and velocity. Ingestion processes determine how data will be consumed (eg when and where is it most secure to stream data for faster, real time outcomes?).
4. Data transformation	During processing, data rules trigger and transform data into a format that is readable by the target (user and/or machines). Readable does not always mean acceptable, however. Rules are created directly within a data integration stream or rely on alternative technologies embedded in or accessible from within a tool. Similar to the power grid converting energy for building and customer usage as assets traverse the network, the same applies to power and associated data as they travel for instance, from substations to marketers.
5. Data storage	The design, implementation and support of stored energy to maximise its value throughout its lifecycle is instrumental in managing energy as a strategic asset. If storage capacity is not increased sufficiently to meet increasing demands this could cause system failure, unintended power spillage or network overload with consequences similar to the NYC analogy. In addition to posing cyber vulnerabilities, data quality issues can surface during storage issues causing business, market and customer uncertainty.
6. Data distribution and provisioning	The dissemination of data to authorised sources for consumption and redistribution, eg DERs. Similar to element #4 energy and data are selected and made available (provisioned) for consumption by specific users and based on ethical and organisational policy. What data is distributed and presented to whom, when, how? What are shut off and de-provisioning guidelines? Transmission lines for power can become compromised and therefore alternate energy sources should be integrated in modernised designs.
7. Advanced data analytics (ADA)	Autonomous or semi-autonomous examination of data or content using sophisticated techniques and tools, typically beyond those of traditional business intelligence to discover deeper insights, make predictions or generate recommendations must be a part of the EDRM and utility ecosystem. Whether energy assets and components are operating normally or abnormally, it is through sophisticated analytics that threat vectors are detected, minimised and ultimately eliminated. The use of geographic, geospatial data provides greater situational awareness and context while machine learning (ML) is applied, for example, to sort and conduct facial recognition of images captured on camera that are unclear to reviewers. AI then augments geospatial and ML suggesting the actor's intentions and impacts on the network. Data and text mining, semantic and sentiment analysis, network and cluster analysis, multivariate statistics, graph analysis, complex event processing, neural networks and geospatial analytics are example ADA capabilities.
8. Data consumption	How data is used is the emphasis. Once ingested, data is utilised and the EDRM provides references based on usage patterns, velocity and demand/supply predictors. Power consumption, demand and peak load assessment are example consumption considerations that based on expected results can indicate threats and/or performance issues.

9. Data classification	Data classification involves tagging and labelling data and metadata so that they are recognised and interpreted. Classification is a necessity as energy data and statistics are used to make investments, invoke alternate power supplies, eg solar or wind renewables, and other decisions. Following are example content, context and user-based classifications: • Personally identifiable information is content based type of classification; • Data signals sent to traffic light sensors in a geographical location to display flashing yellow lights for a period of time due to weather conditions is a form of context-based classification; • Unclassified and for official use only are forms of user-based classification.
10. Data transport and exchange (DT&E)	Considerations for moving data from one location to another is analogous with the power grid exchanging data between storage devices and power sub stations. Extraction, load and transformation processes vary depending on the assets and components in the network. During DT&E, what is most important is that the energy supply does not become compromised.

Appendix A provides a visual description of an EDRM.

ARCHITECTURE — THE FOUNDATION FOR SUSTAINED DECISION MAKING, EVIDENCE BASED POLICIES AND GOVERNANCE

In a previous section, this paper described the importance of knowing and maintaining an inventory of assets, components, relationships and interdependences across the power pipeline and network in order to protect assets against cyber intrusions. Treating energy as an enterprise strategic asset requires situational awareness of the ecosystem, behaviour profiling relative to its purpose, compliance and scenario-based modelling that prepares and responds to good as well as egregious activity. A solid architecture provides a foundation for sustained decision making, evidenced-based policies, and value-centred results. Some modern architectural outcomes are:

- *Secure delivery*: Safe, compliant solutions with a high degree of customer satisfaction through alignment of approved enterprise assets;
- *Interoperability*: Account for unique requirements for broader organisational needs that require federation, preserving organisational autonomy when necessary;
- *Agility*: Recognise and deliver cyber, technology and business policy and innovations through agility and resource flexibility;
- *Informed*: Increase process and cost efficiency through continuous asset management and monitoring;
- *Return on investments (RoI)*: Achieve maximum RoI by eliminating redundancies and applying asset reuse;
- *Coordination*: Components (systems, devices, orchestrators) cooperate via architectural structure[8] to protect assets and solve problems;
- *Feedback*: Apply continuous, dynamic feedback loops, metrics and learnings;
- *Evidence*: Available body of facts.

MODERNISING ENTERPRISE ARCHITECTURE

An organisation's executive leader must strengthen leadership of cyber security protections across the enterprise. They expressed interest in knowing the threat assessment tools and safeguards that are currently operating and protecting bulk grid power. Through enterprise architecture (EA) two candidates were identified that met some of their needs. The leader was able to review total cost of ownership, business impacts and complete RoI analysis — an outcome of EA modelling — concluding that a third cyber

solution be classified as a critical asset and strategically aligned as the standard because it met all of her criteria for an enterprise bulk grid protection solution. EA modelling is both static and dynamic and based on scope. In this example the model exposed a gap in policy for rerouting bulk power in the event of a crisis, an opportunity to streamline work flows was reflected, system redundancy became apparent and the need for greater talent pools in cyber risk management was evident. Figures 2 and 3 illustrate how EA facilitates value-based decisions and furthers support of energy as an enterprise strategic asset.

Dimension 1: Values axis

- All business units should align results with achieving the overarching *mission* of the organisation;
- The *strategy* layer captures primary stakeholders, drivers, goals, and objectives of the enterprise including business strategy, IT strategy, cyber strategy. *Strategy* elements are defined and evolved to directly support the *mission*. Business strategy engages customer feedback and envisions customer experiences to create business value;
- The *intelligence* layer is the foundation for actionable and data driven decisions. Tenets of intelligence are data, insight, foresight and hindsight. *Intelligence* directly supports strategy with data insights driving new strategic direction and objectives for the organisation. The EDRM described in a previous section of this paper is an example intelligence artefact;
- The *compute* layer encompasses agile software development and information technology (IT) operations and practices as well as the technology reference model. Agile methodology ensures an evolutionary practice that is more responsive and adaptive to technological innovation. An agile architecture will support the enterprise in a leaner and more

Scenario – Bulk Power Grid Capability Decisions

Description:
An organizational executive wants to enhance leadership of cyber security protections and response planning, acquiring energy focused cyber tools to monitor and respond to threats against bulk power grid capability.

Using the model:
Using the enterprise architecture model, the leader was informed of numerous instances of tools with energy management capability; one in particular had bulk power system monitoring and communications. Leader assessed change impacts and planned broader enterprise adoption. There were no acquisitions required at the point in time.

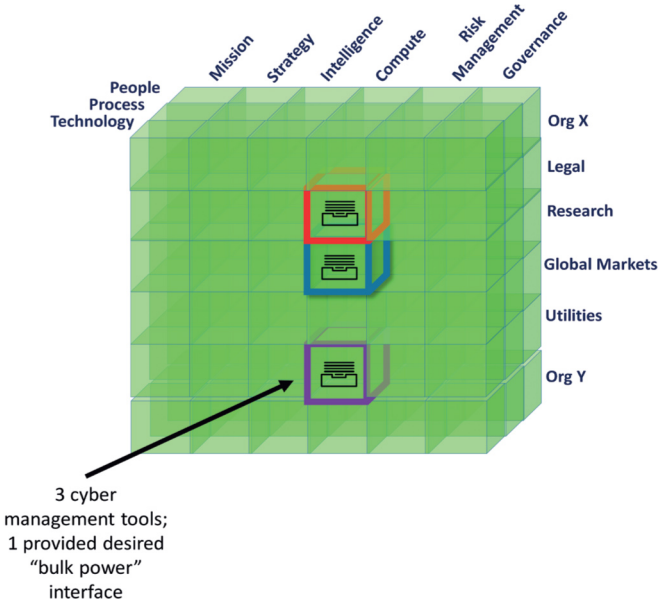

Figure 2: Enterprise architecture model facilitates bulk grid management policy and technology decisions. The three-dimensional EA model's first dimension identifies attributes for achieving valuable outcomes. These are mission, strategy, intelligence, compute, risk management and governance; the second dimension, people, process and technology, are the enablers of value-based decisions; and third dimension is the organisational structure or where the model is applied. In Figure 2, multiple organisations were modelled and viewed cohesively.
Source: Author

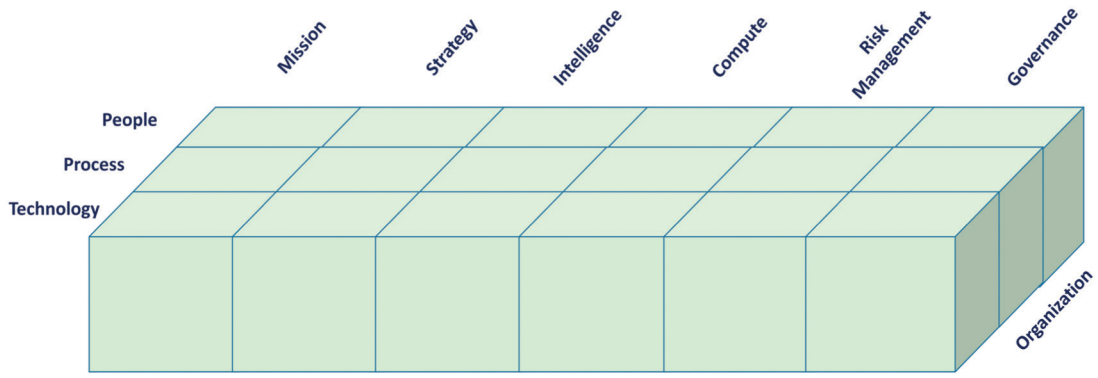

Figure 3: Modern enterprise architecture is incremental, value based and evidentiary, improving cohesive business process and technology decisions. AI, for instance, leverages EA to detect simultaneous hacks on industrial control systems and assess impacts to the energy ecosystem with realistic counter-measures
Source: Author

business-oriented way. *Compute* provides a suite of tools and platforms and upon policy makes available to the enterprise. *Compute* drives *intelligence* by providing the tools and inventory for insight;

- *Risk management* is the layer for secured, sustainable investments, providing control elements in the form of policy, process, asset management and change control. Risk management provides guidance for identifying and measuring the impacts of threats with mitigation and standards as needed. Performance scorecards are derived and maintained in this layer, reflecting the effectiveness of security controls. Scorecards identify gaps and provide mechanisms for ranking, prioritising and mitigating risks;
- *Governance and policy* is the layer that comprises the EA model. Governance addresses the establishment and enforcement of decisions (ie through governance boards and councils). This layer guides and incentivises policy adoption across workforce and leadership.

Dimension 2: People, process, technology axis

- *People*: The people element captures workforce, skill sets, and stakeholders that go into the EA. Workforce culture and human skills and knowledge must evolve as cyber and technological advancements occur, and identifying personnel and defining roles that guide security standards and plans is ongoing;
- *Process*: The process element captures procedures and controls carried by the organisation and its people;
- *Technology*: The technology element puts guidelines, plans, and models in place to support the organisation's people and processes.

Dimension 3. Organisational axis

The organisational dimension provides a map for information discovery and a view into how an enterprise, extended enterprise and business units perform relative to dimensions 1 and 2. The organisational views facilitate the use of EA as a tool to plan and map ecosystem activity such as cyberthreat-hunting scenarios and to validate interoperability. AI leverages EA, for instance to detect simultaneous hacks on industry control systems and assess the cascading impacts across the energy pipeline, preferably before incidents arise.

Collectively, an effective EA provides an enterprise view into the current and predicted performance of an organisation and its subsets. EA modelling offers a platform for scenario and mathematical modelling of

portfolios and is an anchor to effective use and deployment of strategic business and technology assets. This insight fuels effective change management; cyber risk impact assessments; sustained decision-making that for instance, is so valuable it merits persistence irrespective of leadership changes; evidenced based 'trustworthy' policy development based on the needs of an organisation; operationalisation; and governance.

In summary, energy is a strategic asset that organisations can protect through mitigating cyber risks by applying three key principles:

1. Application of zero trust across the entire energy network;
2. Conduct smarter data modelling and smarter data management improving traditional approaches to encompass greater situational awareness with integrated ethical governance;
3. Modernise and approach architecture as the foundation for sustained decision making, evidence-based policies and governance and utilise EA as the foundation for your cyber defence strategy.

References

1. Taft, J. D. (September/October 2019), 'Grid Architecture', *IEEE Power & Energy Magazine*, Vol. 17, No. 5.
2. 'Stunex computer worm', see *Encyclopaedia Britannica*, available at https://www.britannica.com/technology/Stuxnet (accessed 6th November, 2019).
3. Con Edison (July 2019), 'Statement from Con Edison', available at https://www.coned.com/en/about-us/media-center/news/20190714/statement-from-con-edison (accessed 6th November, 2019).
4. Gartner (April 2019), 'Market Guide for Zero Trust Network Access', available at https://www.zscaler.com/gartner-zero-trust-network-access (accessed 6th November, 2019).
5. US Department of Energy (July 2019), 'North American Energy Resilience Model', Office of Electricity, available at https://www.energy.gov/sites/prod/files/2019/07/f65/NAERM_Report_public_version_072219_508.pdf (accessed 6th November, 2019).
6. Pearce, G. (2019), 'CGEIT: Acknowledging Humanity in the Governance of Emerging Technology and Digital Transformation', *ISACA Journal Governance of IT, OT and IOT*, Vol. 4.
7. U.S. Energy Information Administration (October 2015), 'Electric power sales, revenue, and energy efficiency: Form EIA-861 detailed data files', Final 2014 data, available at https://www.eia.gov/electricity/data/eia861/ (accessed 6th November, 2019).
8. *Ibid.*, note 1.

APPENDIX A : ENTERPRISE DATA REFERENCE MODEL – AN ILLUSTRATION