A Comprehensive Tutorial on Data & Cybersecurity

Concepts, Analysis & Best Practices

By Dr. Erfan Ibrahim

CEO & Founder

The Bit Bazaar LLC

erfan@tbbllc.com

1. Introduction:

The electric sector is witnessing rapid transformation globally because of environmental concerns with generation from fossil fuels, growing demand from consumers for clean energy choices and deregulation. At the same time advanced digital technologies are entering the electric sector to improve energy efficiency, integrate increasing amounts of intermittent renewable energy and improve command and control functions farther out on the electric grid. All these changes do come at a cost - a more intelligent and networked grid also opens new cyberattack surfaces that can be exploited by a variety of hackers with different motivations.

While the CIP compliance requirements from NERC and the cybersecurity requirements from standards such as NIST 800-53, IEC 62351, NIST CSF and DoE C2 M2 are attempting to address the cybersecurity challenges that today's power systems face, they do little to address the risks from insider hackers and Advanced Persistent Threats coming from nation states and nefarious organizations. The requirements are either too high level with plenty of wiggle room and leaving vulnerabilities in power systems or they are IT centric and assume the hacker is on the outside and does not have access to the security controls that protect the power system devices.

You must be wondering how I can make such sweeping generalizations about the limitations of major cybersecurity standards from IEEE, IEC, NERC, NIST and DoE. It is simple. I have been in the electric sector for over 10 years, after 12 years in telecom, networking and cybersecurity and looked closely at these standards and proved their short comings to the insider threat in a power system cyber testbed I designed and built at a major US National Lab from scratch. We succeeded in getting past all the authentication schemes, encryption technologies and role-based access controls that these standards recommend by launching attacks from within. I found a more effective way to protect IT and OT networks that has not been compromised in three years by Red Team testers.

2. The Four Functional Layers of Cybersecurity:

I would encourage you to view cybersecurity in 4 layers.

The first layer is confidentiality enforced by authentication, role-based access control and cryptography. This limits legitimate users access to data based on their role or need. All other data is either inaccessible by privilege rules and/or encrypted so it cannot be used without formal authorization. Firewalls with remote logins via Virtual Private Networks between remote users and corporate firewalls, block or selective encryption of data in the enterprise, access control lists on switches limiting data traffic between network nodes, username/password lock on IT or OT applications and digital certificates for authentication fall in this category.

The second layer consists of intrusion detection and prevention with malware signatures. This is used widely on the IT side of corporate networks and increasingly on OT networks that are moving to the TCP/IP protocol and prone to malware originating from the public Internet. There are many commercially available products in this space.

The second layer of security includes intrusion detection systems from Cisco, Juniper, NexDefense, N-Dimension and several others. You could include FireEye and Palo Alto Networks appliances in this category. Products like N-Dimension go a step further and include signatures for malware from power systems SCADA protocols such as DNP3, IEC 61850, Modbus, OPC, etc. NexDefense looks for anomalies in network connections and ports serving specific applications from certain IP nodes and alarms when there are violations relative to expected network connections and protocol traffic between IP nodes. All this is situational awareness. Palo Alto Networks and FireEye use pattern recognition of cyberattacks to develop near zero-day attack protection for IT type malware proliferation.

The second layer is sufficient for IT security situational awareness and some nefarious behaviors on OT networks that leverage Internet based malware (e.g. precursor to Black Energy attack in Ukraine). Tomorrow's post will go into the 3rd layer of security - context based intrusion detection that is protocol based.

The third layer of security is derived from context-based intrusion detection and prevention. This is provided by a combination of intrusion detection systems that can sit on inline taps or hardware layer filters that allows certain commands and values in a messaging protocol to get through and block others based on rules set up in advance by the operators. The context-based IDS systems in this case understand the semantics and commands of the protocols that they are observing and check the messages and values relative to a set of rules set up by the operator.

The third layer of security is critical to protect against the insider threat or Advanced Persistent Threat that have stolen the access control credentials of the power systems and are performing nefarious activities on a power systems device or a set of them with deep domain expertise to make their hack subtle. It could be as simple as giving bogus values on legitimate commands, disrupt systems or exfiltrate data. Since this type of hack does not come with any malware that has a signature, the typical IT type IDS systems that we covered in Layer 2 of security cannot catch such hacks. Products from Albeado, SUBNET and SecLab fall in this category. Others include CyberX, WaterFall Security, Indegy, Radiflow, etc.

The 4th layer of security is endpoint security. This includes firewalls in VMware like hypervisors, firewalls at the OS level either directly installed on hardware or a VM instance with an OS, username/password on the application, encrypted data stored on the end system with select keys for certain data fields and tamper resistant software that alerts if the host application gets compromised and auto ejects from the network, so it does not become a pivot for a wider cyberattack.

Endpoint security in power systems can go further into the realm of non-networked security. At the microprocessor level the power system node is programmed to only accept certain commands in the SCADA protocol based on its function and reject others. If the state of the system starts moving in the wrong direction there is a self-restoring force in the endpoint to return to an acceptable range of values for variables like voltage, current, and phase. It is non-networked because this logic is programmed into the microprocessor and cannot be altered remotely. This is critical to protect high value power systems

assets that could be targeted by insiders and/or APTs. Check out DoE CODEF project to see an example of such built-in security in power systems. Also search Variable Oscillator Controller (VOC).

3. **Building A Cyber Aware Enterprise:**

Shifting the focus from concepts to synthesis - cybersecurity in enterprises is getting very complicated because of the rapid proliferation of digitalization in every aspect of business process is bringing many users and systems into the digital network each with their unique function and potential attack surface. To get a proper grip of the cybersecurity posture, an organization needs to bring the business process architects, the cyber architects and network architects into cross cutting teams to develop use cases, network and security requirements, overall logical architecture and implementation strategy so everyone is on the same page and the cybersecurity posture and network design evolve based on business needs and potential threats.

This takes bold moves on the part of the senior management to reorganize their enterprise to create such crosscutting teams. We can no longer afford to operate in silos when the cyber threat is fully integrated and exploits the cracks in business process, network design and security.

4. **Pros & Cons of the TCP/IP Protocol:**

Pros: TCP/IP provides services like IPsec and TLS that provide obfuscation of data during transit. TLS uses end-to-end encryption and authentication. With IPsec encrypted tunnels can be established between routers or end-users and firewalls. Both TLS and IPsec are good to protect data in transit from man-in-the-middle attacks. Another benefit that TCP/IP protocol provides is the logical separation of the upper layers associated with the application from the lower PHY/MAC layer considerations. This modular architecture allows TCP/IP based applications to be developed without concern of the underlying hardware that will transport their data.

Con: TCP/IP protocol security controls do not have any means to protect against the insider threat that has the TLS authentication credentials or is present on the clear text side of the VPN tunnel. It assumes the hack is external to the network. This is a huge vulnerability now because of the insider threat from disgruntled employees and Advanced Persistent Threats.

Pros: TCP/IP provides you a universal addressing scheme for network nodes that is not dependent on the underlying hardware specifications. It is simple to create logical subnets in TCP/IP for segmentation of the network by business function. Through access control lists on routers/switches, it is easy to restrict access between IP nodes in these subnets based on need (i.e. justified by an authorized use case). This is the essence of role-based access control. VPN logins on firewalls from remote connections is another way.

Cons: Hackers can spoof known IP addresses from laptops and get past the role-based access control policies on switches. Additionally, TCP/IP requires the 3-way TCP handshake to be completed before IPsec and TLS type services are rendered. That is too late. Advanced Persistent Threats and insider threats can make repeated TCP connect requests from rogue IP addresses assigned to laptops connected to router/switches and launch DoS attacks at will.

5. **In-line Blocking Technology Example for DDoS Protection:**

I will now describe a commercially available cybersecurity technology that mitigates the challenge of spoofing and DDoS attacks in IP networks by using security tokens in the TCP header to provide application layer security at the TCP layer.

The technology I am referring to is Blackridge. It is an appliance based or embedded software technology. It sits in-line with one appliance in front of the source and another appliance in front of the destination. As data packets travel from the source to the destination a token is inserted in the header of each TCP segment by the Blackridge appliance in front of it. Before each data packet is delivered to the destination the Blackridge appliance in front of the destination validates the token in each TCP header. If the token has expired or is missing the entire data packet is dropped by the Blackridge appliance in front of the destination.

Blackridge offers appliances with 1 Gb and 10Gb throughput. The tokens are synchronized by encrypted transmission out of band via management VLAN (logically separated from application VLAN). The token only last 4 seconds. Spoofing from a laptop cannot get past the Blackridge appliances because the tokens are missing in their data traffic. DDoS attacks get repelled by the Blackridge appliance up to 10 Gb speed. If the token is stolen and inserted in a packet it will be out of sequence and dropped. I proved its viability in a power systems security test bed at a major national lab.

6. Importance of Protecting Network & Business Process Layers:

To protect critical infrastructure on digital networks we need to place appropriate security controls at the business process and network layers as well as configuring security controls provided by purpose-built cybersecurity technologies or the embedded security controls in the command and control protocols.

Unfortunately, this is not really happening to protect critical infrastructure today. The obsession of enterprise security on authentication and encryption is overshadowing the need to limit access between nodes with granular access control lists on switches and routers. Furthermore, IDS systems are being placed across the IT/OT network infrastructure but most of them are signature-based malware detection types that are blind to data fuzzing and disruption from insider threats or APTs.

While business lines are analyzing use cases in granular detail for productivity, the network and cyber community are simply opening and shutting access to nodes based on demands from these business lines without truly comprehending the use case transactions at the business process layer and their cybersecurity implications. This is like manna and quails for the sophisticated hacker. It is time to change this myopic mind set and think holistically.

7. The Role of Cyber Governance Assessments:

A holistic approach to cybersecurity is needed for any enterprise that has digital technologies deployed for business operations. It starts with a cyber governance assessment of each business unit that has a distinct cybersecurity maturity level. An enterprise could assess the IT, Control Systems, Telecom and Broadband separately. The assessment is based on identifying which business process security controls from the DoE Cybersecurity Capability Maturity Model (C2 M2) and NIST Cybersecurity Framework (CSF) have been implemented and which have not and the order in which the missing controls need to be implemented (highest to lowest priority).

Cyber governance assessments have been reduced from a manually intensive exercise taking days down to a 6-8 hours exercise using an automated software tool that I helped develop and use with my consulting clients. The tool integrates the two frameworks into a single assessment and saves enterprises money, time and unnecessary contention.

Let us dig a little further into the value of cyber governance assessments. If an enterprise has done a complete job of identifying which business process security controls they have implemented across the 10 domains of the DoE C2 M2 and the 5 categories of NIST CSF in each of their key business units with a consistent cybersecurity posture and which controls they have not implemented, the C-Level, the manager level and the technical staff can view the cybersecurity maturity level of their business units from a common perspective and fill the gaps as a team.

Why is this alignment important? Because it is the first step towards aligning the IT and cyber goals of an enterprise with their business goals. Furthermore, it creates the right business rationale for making specific investments in technologies, core process re-engineering, new policies and workforce development to protect the enterprise against the dire consequences of data breaches. Each infrastructure project is informed by a standards-based approach to securing the overall enterprise. In some cases, the activity could be as simple as creating a logging spread sheet. In other cases, it could mean upgrading firewalls, creating an alarm visualization capability or tracking HW/SW and IT services across the enterprise.

8. The Shortcomings of Cyber Governance Assessment Freeware:

The challenge with using the free tools available for doing cyber governance assessments is that they are not only manually tedious they cannot prioritize the missing business process security controls into a plan with measurable labor, technology and funding sources. Many enterprises have gone through the painful exercise on their own and with government and private sector entities and were left less than satisfied. This is unfortunate because the DoE C2 M2 and NIST CSF do have valuable guidance to secure enterprises from a top down perspective.

After overseeing 20+ cyber governance assessments of electric utilities across the US in my last job using the automated software tool that I helped develop, I discovered that most of the utilities assessed did not have adequate controls for risk management strategy, asset and configuration management, and workforce development. In many other C2 M2 domains they had several controls at the ad hoc level. In my new role leading TBB CEO Consulting, I am approaching utilities and other enterprises with my team and offering cyber governance assessments with the automated software, so I can develop proper project plans for their missing business process security controls with an eye on priority, threats and funding.

9. The Top 10 Recommended Priorities for a Chief Information Security Officer (CISO):

What are the top 10 things a CISO should do to get a handle over the cybersecurity posture of their enterprise quickly?

- Perform a set of cyber governance assessments of their key business units to identify the missing business process controls.
- Put cross cutting teams to build technical implementation plans to fill the missing controls.
- Get budget approvals for the implementation plans from the CFO

- Walk the entire digital/analog infrastructure with their cyber and network teams and document all the HW, SW, patches, physical and logical connectivity and enter it into a proper asset and configuration management tool
- Review the business use cases that run on the infrastructure to ensure that the network configs and cyber controls only allow data traffic of the approved use cases
- Audit every network segment with Wireshark packet capture to ensure purpose
- Develop a proper identity and access management program and map it to the network and security infrastructure discovered with the walk through
- Train the network and cyber team to work together and link their salary bonuses to tangible metrics of collaboration
- Keep the C-Level management updated on the activities and continually seek their buy in
- Attend at least 3 industry events per year for subject awareness

10. The Changing Role of a CISO:

In my humble opinion, the traditional role of a CISO within an IT organization reporting to a CIO is ineffective today. I also think the "I" in CISO title is limiting. As physical, cyber and EMP threats to the infrastructure of an organization increase we need a Chief Security Officer reporting to the COO to be the true visionary establishing an "all hazards approach" to security.

A physical security director, compliance director and an information security director should all report to the CSO. The network director should also report to the CSO. The CSO should be a peer to the CIO who also reports to the COO. The CIO should focus primarily on the information systems supporting the business lines and work with the CSO and their information security and network director for role-based access control.

In this way, the COO has a true handle on an organization's operations by having all the IT assets supporting key business functions by the CIO and all key aspects of network, security and compliance by the CSO under their supervision to ensure business continuity, productivity and cost containment. The COO should empower the CIO, the CSO and the business units to collaborate to build cross cutting teams to ensure compliance with standards, business efficiency and security.

11. The Real Role of a CIO:

To elaborate on my last post, I am not trying to diminish the role of a CIO. I am advocating a new focus of the CIO based on their actual skill set. Most CIOs in thriving organizations are highly stressed individuals with too much on their plate and not enough time to do justice to any of their key job functions. The CIO is responsible for everything and not recognized for anything. Whether it is the network, security, application or data, if the end user has an issue the CIO's team is the first one that is blamed. It is very hard for a CIO to keep up with the pace of development in networking, security, application and data management simultaneously. They are often resource and labor constrained and their relationship with the CFO can be quite contentious.

What is the real value of giving so many responsibilities to the CIO when they are overwhelmed, under resourced and often scapegoated? If a CIO was just made responsible of generating, collecting, organizing and analyzing all the data of an organization to support the business lines and left security

and networking to the CSO they would be far better off in their job and receive praise and support of the other departments. The CIO can plan better and get CFO buy in. It is time to rethink the role of the CIO.

12. The Data Deluge Challenge in Enterprises:

The digital revolution has affected all aspects of any enterprise today. Data is being exchanged with external entities over the Internet and/or private networks for business transactions, research, social networking and public relations. Data is also being exchanged among the various departments of an enterprise for day to day operations. There are several different data types traversing the network with different frequencies, formats, and sizes.

All this data needs accounting, security, parsing, storage and backup to keep any enterprise running smoothly today. The challenge is that the volume of data is growing faster than the evolution of tools to account for, secure and parse the data. Storing and backup, however, is growing as fast as the volume of data.

The result is that enterprises are growing more intelligent each day without becoming equally smart. That sounds counter intuitive. But if you look deeper you will see what I mean. Intelligence is based on how much data you have stored. Smart is about turning the data into actionable intelligence. That comes from accounting for the data types, ensuring the integrity of data collected and parsing the data and using analytics to derive business significant meaning from it. We are way behind in this area.

13. The Value of Context in Data Security:

Digital data without context is simply a string of 0s and 1s. You get context by knowing the business use cases that created the data. The use case is based on a well-defined transaction between two actors (two machines and machine/human). The use case provides the criteria for the data variety, volume and velocity. Deep learning algorithms can use data with context for veracity.

Keeping a close eye on data in the context of the use cases and the configuration of the network is an effective way to know when the data is accurate and when it has been altered. This enables an enterprise to have effective situational awareness, incident response, information sharing and communications across its IT/OT infrastructure.

If you don't have a precise expectation of data variety, volume and velocity relative to your use cases, the deluge of data from high volume of business transactions will leave you blind to cyber breaches from data fuzzing and/or theft.

Authentication, encryption, anti-virus and access control are certainly part of the layered cyber defense architecture. But data tagging, integrity and anomaly detection are critical for data protection. Flexible data anomaly detection tools are needed to discover subtle data breaches by sophisticated hackers today.

14. Example of Data Context in Anomaly Detection:

To provide a tangible example of context for data let us take the PV smoothing use case that stabilizes the varying voltage from intermittent solar power. A cloud cover can cause the voltage from a solar array to sag instantaneously. In the PV smoothing use case the solar array is connected to a micro grid

or a utility grid with electric storage, the inverter with the solar array can send a control message to the micro grid controller or the SCADA controller in a utility substation reporting the voltage sag. The controller sends a secondary control message to the inverter attached to the electric storage unit to discharge at the same power rate as the solar array power loss rate to keep the voltage constant.

This is how the PV smoothing use case is designed to run in micro grids and grid attached solar. However, suppose an insider threat or Advanced Persistent Threat creates and installs a Python script on the controller that multiplies the power data value from the solar panel by a factor X before sending it to the electric storage. Suddenly there is a voltage surge or drop. There is no malware with signature for IDS to detect. Incoming and outgoing message data values need context in this use case to determine an anomaly has occurred.

15. The Importance of Business Process Security:

In the scenario described above, a business process security technology is required that will read the incoming and outgoing data packets in the command and control protocol (i.e. Modbus, DNP3, OPC, IEC 61850, etc.) relative to the PV smoothing use case and determine the discrepancy in the 2 values.

Since there is no malware or malicious command being communicated cybersecurity appliances from FireEye and Palo Alto Networks will be ineffective to catch this anomaly. IDS from Cisco, Checkpoint and other major vendors that rely on signature-based malware detection won't work either.

Several of the so-called OT security tools in the market that are protocol savvy will also not catch this anomaly because both incoming and outgoing commands are well posed. This is the true nightmare scenario of the insider threat that is being largely ignored in the energy sector today.

A simple Python script added to the logic of a substation SCADA controller can cause the voltage to surge or get depressed to the point where IEEE 1547 standard would force the DER asset to disconnect from the grid due to poor power quality. Fortunately, there is a software tool from Albeado called PRISM that can flag such anomalies in power systems and allow the operator to take corrective action.

16. The Logic Behind Cybersecurity Breach Explosion in Enterprises Today:

Why are so many cybersecurity breaches happening globally? There is no shortage of CISSP's, cybersecurity conferences are overflowing with vendors claiming panaceas, consultants are offering endless cyber services to shore up defenses of enterprises and new State and Federal cybersecurity regulations are being shoved down the throats of asset owners like fiber supplements.

I think it is because we are approaching cybersecurity the wrong way. We have a defensive instead of an offensive mindset. We want to put up barriers against the hacker without understanding the thought process of the hacker or their modus operandi. Ask anyone with a top US security clearance who has done cyber penetration work for our nation for a living. They mock the so-called cybersecurity controls that exist in most enterprises today after millions of dollars have been spent doing assessments and implementing controls to protect against external threats.

The challenge is not technical but human. Processing speed, expediency and easy access after some level of authentication are the driving forces behind most IT/OT network designs today. These are all red carpets for the insider threat or Advanced Persistent Threat that leverages these features to cause harm.

17. Analyzing the Roots of Enterprise Security Dysfunctionality:

Let us delve deeper into the dysfunctional aspects of enterprise security today and explore ways we can correct them. The first is an obsession with mathematical complexity and the use of high speed processors to manifest it in every digital transaction we can shove it into.

What do you expect when you will seek inspiration for security architectures from math and computer science majors? This is their academic training. Just like people who graduate with a degree in "medicine" prescribe medicine for everything instead of looking holistically at a patient for cures, mathematicians and computer scientists revel in quantitative complexity to solve any problem. Academic research encourages a pissing competition between their graduate students in complexity and anoint them with advanced degrees based on this complexity and obscurity rather than practicality.

Investors enable these "geniuses" further by funding to bring their obscurity to market. RSA, RedHat and Defcon become their coming out parties to dazzle the layman with their security "Towers of Babel (babble?)". The problem is that the hacker has also had the same training and can outwit these INTP geniuses by going around their complexity.

18. The Futility of Complexity in Data Security:

I am being deliberately provocative and incendiary. It is meant to get you out of your mental models of information technology and how cyber vulnerabilities need to be addressed. I have the highest respect for the intellectual acumen of math and computer science majors and understand deeply what they contribute in our digital age.

I know complexity well. I am a plasma physicist by academic training and was solving coupled Maxwell's equations in million+ line Fortran 77 plasma simulation codes as early as 1984 at Lawrence Berkeley Labs as a 20-years old Nuclear Engineering PhD candidate at UC Berkeley.

I also know the futility of complexity when it is applied unnecessarily. This is one of the reasons why we may never see a practical fusion reactor in our lifetime no matter what MIT, Lockheed, ITER and the Japanese are claiming. The poor magnetohydrodynamics associated with a doughnut shape magnetic bottle can never be overcome by all the engineering complexity of super magnetics trying to confine it.

This is the reason why 27 years after I left the field of fusion engineering, we are still hovering around the breakeven point billions of R&D dollars later. The same is the case with cybersecurity. Complexity only creates false positives and renders the security technology ineffective. Moores Law needs guidance!

19. Moore's Law – A Key Driver of Complexity in Data Security:

Moore's Law says that the processing speed doubles every 18 months and the price of memory drops by 50% every 18 months. The rule has held for several years. Network bandwidth limits are growing steadily, and the cost of communications is coming down. Combine that with the development of virtualization in computers and big data structures (e.g. Hadoop clusters) over the past decade and you have all the 11 herbs and spices for cloud computing!

All this leads to complexity. Data fuzzing by the insider threat is the Achilles Heel for this complexity. Since 7 out of 10 cyber threats are insider today we cannot ignore it. Confidentiality alone does not cut

it. So, while many pundits in the industry will brag about the air tight security of cloud computing they are evasive about how secure your data is in the cloud.

The insider threat could be local to your enterprise or work for the cloud company. The complexity of the data infrastructure in the cloud does not secure your data - you do! By securing I don't mean encryption. I mean monitoring the data relative to the protocols and business processes running and determining its integrity, accuracy and availability in real time I will now describe an alternative cyber architecture that can embrace complexity without sacrificing data security.

Complexity is not a through street for cybersecurity no matter how much centralized informatics we introduce with cloud computing driven by Moore's Law to detect anomalies at the edge. This is a profound observation that the cybersecurity community is largely ignoring these days because of their obsession with high speed processing, broadband networks and big data creating centralized intelligence architectures.

20. Mitigating Complexity in Data Security with Distributed Intelligence & Computing:

I think the farther you are from a network node, the less likely it is that you can detect an anomaly at that node and respond to it in real time. This is not because of data transit time. The issue is the farther away you go from a node the more degrees of freedom exist in the network and the more computations you need to perform to determine an anomaly with confidence. The exponential rate of increase of data elements to consider for anomaly detection away from the observed node is faster than the rate of increase in computational speed at the higher level to detect and respond to the anomaly. Unbounded problem!

The solution is a hybrid model of distributed intelligence and computing at the edge for real time anomaly detection and response and centralized computing with summary data from the edge for deep learning and long-term risk mitigation.

Form factors and price points of computing are shrinking to the point where it is feasible to inspect data packets reliably at the edge of the network and detect anomalies locally. This is where well-defined use cases are running with few degrees of freedom and clear expectations of volume, variety and velocity of data to ensure veracity of data in a scalable way. This is a bounded problem because computation scales with complexity locally.

Legacy power systems computational capability is not necessary for data inspection at the edge. Commercially available data packet inspection tools can monitor critical network links to inspect and detect anomalies. Edge computing cost may be higher initially compared to centralized cloud computing. But due to the effectiveness of edge security to rapidly identify and block the hacker from getting a foothold, edge wins easily over central in real time threat identification and mitigation. Centralized computing breaches in the future will make the economic case for edge computing.

Remember, complexity is the hacker's best friend. Centralized computing with the cloud has its place in long term cyber risk assessment. Edge computing is the more scalable and effective real time threat detection and mitigation option. Food for thought.