Electricity: The Most Critical Of Critical Sector With Cyber Risk

*By Sai Huda, author, **Next Level Cybersecurity***

When it comes to cyber risk, electricity is without a doubt the most critical of critical sectors. Imagine if all of a sudden there was no electricity for several days. What if it was for several weeks or longer. It would be catastrophic. Just about everything, everywhere would come to a halt.

It would cause severe economic, health and environmental damage. In the U.S., just in the east coast, Lloyd’s of London estimates $243 billion in insurance costs and loss of life and damage from a cyberattack disrupting the electricity distribution network.

Bad actors such as organized crime groups and rogue nation-states know this and are going after the electricity sector with more cyberattacks than ever before.

They are also targeting the supply chain first, to infiltrate and use as the “backdoor” into the electricity sector. So not only are the 3,300 electricity utilities in the U.S. prime targets, so are its suppliers.

In my book, Next Level Cybersecurity: Detect The Signals, Stop The Hack, in one of the cases, I show how a rogue nation-state broke into several “staging targets” first. These were suppliers. They used the suppliers as the “back door” to break into the electricity utilities to steal detailed information about the Crown Jewels (i.e. mission-critical cyber assets and systems) to plan the eventual attack on the utilities. The book shows what a cyber attack chain is and reveals the common signals to look for to detect the attacker timely, regardless of whether you are an electricity utility or other type of entity.

The U.S. President’s National Infrastructure Advisory Council (NIAC) warned in its December 2018 **“Surviving a Catastrophic Power Outage”** Report that:

“…existing national plans, response resources, and coordination strategies would be outmatched by a catastrophic power outage. This profound risk requires a new national focus…”

The North American Electric Reliability Corporation (NERC) in January 2019 also sent a warning to the electricity sector and raised the bar for cyber risk management by assessing a $10 million penalty for 127 violations of cyber security standards by a electricity utility.

NERC determined that the violations in aggregate created serious and substantial risk, and mandated cybersecurity enhancements.

The Federal Energy Regulatory Commission (FERC) also approved new cybersecurity standards on security management controls and supply chain risk management that utilities must comply by January 1, 2020 and July 1, 2020, respectively.

Electricity utilities must be proactive and not get caught by surprise by either a cyberattack or a regulatory audit. The stakes are too high.

A regulatory audit discovering non-compliance can be costly, but a cyberattack will be even more costly. Just one successful cyberattack on one utility or a supplier can cause a domino effect and lead to a systemic catastrophe.

So what can electricity utilities do now? Take the below five minute, five question risk assessment.
If you answer No to any of the questions, you have unmitigated risk and must take action immediately.

Electricity Utility Five Minute Risk Assessment

1. Have you performed a self-assessment, comparing the violations in the January 2019 precedent-setting $10 million notice of penalty case to your utility, to make sure you do not have similar violations and exposures? Yes No

2. Have you performed a mock regulatory audit to prepare for your upcoming regulatory audit and addressed any non-compliance, gaps or blind spots before the audit? Yes No

3. Have you trained your entire organization using three tiers (oversight, awareness and performance) and on the cybersecurity standards, beyond basic security awareness, to prevent non-compliance as happened in the $10 million case? Yes No

4. Are you performing ongoing Crown Jewels Threats and Vulnerabilities Risk Assessment, to make sure you not only correctly categorize low, medium and high impact cyber assets and systems but also map to threats, vulnerabilities and risk mitigation, including monitoring for signals of cyber attackers trying to get to the Crown Jewels, and report results to the board for ongoing oversight? Yes No

5. Have you analyzed the new security management controls and supply chain cybersecurity standards that become effective January 1, 2020 and July 1, 2020, respectively, to identify action steps necessary for compliance and implemented a plan to attain timely compliance? Yes No

About the Author

Sai Huda is a globally recognized risk and cybersecurity expert, technology visionary and business leader, with more than 20 years of hands-on experience.

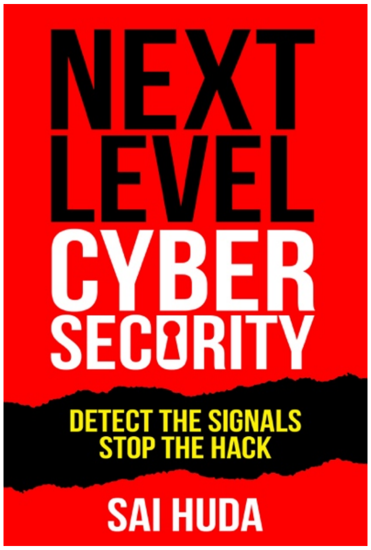
He is the best-selling author of the game-changing book, ***Next Level Cybersecurity: Detect The Signals, Stop The Hack***. It is a book like no other. It is based on intensive reviews of the world's largest data breaches and ransomware attacks and reveals the secret to cybersecurity success – detect cyber attackers' signals early.

The book shows what those signals are and how to detect them in time to prevent loss or damage.

He served seven years as General Manager, Risk, Information Security and Compliance Solutions at Fidelity National Information Services, Inc. (FIS), a Fortune 500 company serving more than 20,000 clients globally. Under his leadership, FIS attained number 1 ranking in Chartis RiskTech100®.

Prior to FIS, he was the founder and CEO of Compliance Coach, Inc., an innovative company providing risk management software and consulting services to more than 1,500 clients in financial services, healthcare and government sectors. Compliance Coach helped clients manage Information Security, Operational and Compliance risks. Compliance Coach was acquired by FIS.

He serves as an expert consultant to boards and executives on risk and cybersecurity best practices. He is also a frequent keynote speaker at industry conferences. To find out more, visit the author's website at www.saihuda.com. To obtain his book, ***Next Level Cybersecurity***, please visit Amazon.



NEXT
LEVEL
CYBER
SECURITY

DETECT THE SIGNALS
STOP THE HACK

SAI HUDA