Question: The National Institute of Standards and Technology (NIST) recently released its 'Framework for Improving Critical Infrastructure Cyber Security'. For those who are not involved in cyber-security or cyber-defense on an active basis, could you elaborate on what this document aims to achieve and improve upon? Further are there gaps in protecting critical energy infrastructure that are not addressed in this document? If so, how would you propose that these gaps be bridged?

The NIST Framework for Improving Critical Infrastructure Cyber security provides a general approach rather than a step-by-step plan for critical infrastructure providers. It serves as a common language for describing security concepts like "security posture" and "target state" but much of the language is focused on a set of concepts that have already been acknowledged in the industry, such as identifying your sensitive data and strategizing how to secure it.

The NIST framework was necessary but not sufficient. It fails to help individuals quantify their risks because it is more of a generally applicable framework than it is concrete guidance. What's lacking is a much-needed step-by-step plan that outlines exactly what critical infrastructure providers should do to identify and secure data. For example, for each of your storage servers, organizations should identify a backup strategy and create an inventory of individual workstation storage to be better prepared when a breach occurs. Precise, applicable guidance is still very much needed.

Another concern worth considering is that frameworks in general can oftentimes serve as checkboxes for security teams. Once a team has checked a certain box, they feel their goal is accomplished, which can perpetuate a false sense of security. Critical infrastructure providers must remember that security means to continually assess and respond to risk. It is an ongoing process, not a one-time deal.

At the end of the day, the NIST framework is a response to the Administration's executive order focused on creating a more solid plan of national defense. While it serves as a framework encouraging critical infrastructure providers to secure their networks, it does not have the regulatory authority needed to make these guidelines required rather than voluntary. What we have here is a recipe that serves as the perfect starting point, but there is still a lot left to be done.

Question: As our discussion is focusing on the cyber-critical infrastructure link, I'm wondering what event or events that have occurred recently either in the US or abroad point to these vulnerabilities as exercised or exploited by cyber-terrorists?

The hackers that stole 40 million credit card numbers from Target came in through compromised equipment from an outside HVAC vendor. This is exactly the sort of attack critical infrastructure providers should be weary of because this represents a trusted party creating a level of security that was ultimately compromised.

Providers must scrutinize the connections to their networks, as these can be the most vulnerable points within the organization. You can't rule anything out. Until the Target breach, HVAC system connections were considered benign, and now everyone is paying close attention to them. Critical infrastructure providers must ask themselves, what else exists on my network that I don't think about frequently could cause an equally as catastrophic data breach as what happened at Target?

Question: To change the line of questioning slightly, there is a lot of talk about the Internet of everything. Now as a home owner and consumer, I'm aware of the proposed 'positives' of everything being internet-routed from being able to control the temperature in my house to turning off and on lights when I need them. I'm also aware of the downside of the Internet of Things (IoT) when, for example, my wireless connection goes down and I can't even listen to my (wireless) radio. What are the positives and negatives of the IoT for critical infrastructure providers? Presumably we wouldn't be moving in this direction if there weren't positives, but what new vulnerabilities may emerge that provide a darker, downside to critical infrastructure providers?

The problems associated with the Internet of Things are countless. Individuals often don't know why it is a good idea to pick a secure network key for their wireless routers so most will simply set the network key and the main administrative password to one that is easy to remember. We'll soon see the same happen with refrigerators, thermostats, light switches, washing machines, and the like.

Now imagine a DDoS attack in which 10 million refrigerators are hacked and kick on at exactly the same time or all electric heaters in an area are turned on at the same time. This will cause load shedding and lead to blackouts. It may sound like a scene out of a Die Hard movie, but this is the future. If we take this a step further, let's imagine this sense of vulnerability in scenarios in

which remote garage door openers and security systems are compromised, granting access to buildings. Now you're no longer just talking about personal homes, but also offices, places of business and even schools.

What the Internet of Things does for everyone – not only critical infrastructure providers – is create network vulnerabilities that didn't exist before. The more devices connected to network, the more points of vulnerability, which if compromised exposes the entire network.

Question: News reports about a sniper attack on a Pacific Gas & Electric's (PG&E) substation in California last April are raising questions about the vulnerabilities of the U.S power grid. When it comes to terrorism, cyber security isn't the only threat – it's incredibly important, but so is physical security. How will this affect the future of utility security?

What happened at PG&E in California is troubling, and certainly goes to show that cyber threats are not the only real threats utility companies face today. The good news is that a coordinated, well-orchestrated physical attack against the power grid requires a great deal of resources, including personnel and weaponry. Moreover, physical attacks can oftentimes be easier to stop in their tracks than cyber attacks. If a group of individuals are shooting at a physical target, the authorities will be alerted and return gunfire will soon take effect, leading to the halt of the attack. While a coordinated physical attack can put a lot of people out of power, the scale of the operation required to take down as much as a cyber attack can, is enormous. A single attacker in cyberspace might be able to shut an entire provider off, but to conquer the same feat through a physical attack would require an army.

In the case of the recent Target data breach, a single vulnerability through the HVAC system provided access to several thousand computers linked to cash registers as opposed to just one cash register. If you make the same comparison on the physical versus cyber front with regard to the smart grid, you're looking at one versus hundreds if substations being compromised. A lot less effort and risk is required for this type of attack as opposed to physically shooting down a utility provider as well, since a cyber attack can be conducted from anywhere in the world. While it's important to keep in mind the physical security risks, it's even more imperative that utilities have their cyber security defenses in place, as these types of threats are more common and have more far-reaching consequences.

Question: What is the role that private industry is providing in pushing forward cyber-security solutions and how willing is industry itself to invest in these solutions? In answering these

questions I'd like you to keep in mind that the ownership structure of US utilities varies somewhat, and sometimes dramatically, from other areas in the world where utilities are either partially or entirely owned by government.

Much like any other for-profit business scenario, customers prefer their utility bills to be lower, rather than higher, which means providers are sensitive to anything that could incur an extra cost that affects their ability to build a larger network of customers and dominate a market. This often causes companies to take bigger risks than they should when it comes to cybersecurity by not investing in the appropriate forms of defense to keep operations costs down, prices low for customers, and revenues high.

The critical infrastructure industry needs a minimum level of security set in legislation, much like what we have for other industries – Payment Card Industry (PCI) data security standards for the financial / payments industry and the Health Insurance Portability and Accountability Act (HIPAA) information privacy law for the healthcare industry. We also need to hold companies accountable for data breaches. For example a healthcare company can be held accountable by being fined or sending its executives to jail if their healthcare records are breached. I have no personal say in what these specific consequences should be for critical infrastructure providers should be, but the concept is needed in this industry too.

Moving forward, we'll likely see the government create a set of rules that require distinct different security classifications for utility employees very much like what we have in the government. Segmenting user access will mitigate risk and protect against insider threats and creates security barriers between different substations so that if one goes, not all go down. The flow of communication between substations should be one-way, because if these substations communicate with each other, you risk overload conditions.

Question: In closing, to what extent is, or perhaps should, the discussion of cyber-security from threats and challenges to solutions be globalized? Is there a role that international organizations might be able to play in facilitating the discussion of cyber security and critical infrastructure protection and to what extent do you think industry and solutions providers would be willing to engage in such a process if it was put forward?

Global cooperation in facilitating cyber security and critical infrastructure protection is a huge request. Suppose we all agree on a certain set of rules and regulations on how to secure critical infrastructure, and while some countries follow, others don't. How can we truly enforce

something like that? You can't sue a Canadian utility company in a court in New York.

Global legislation would be incredibly difficult to agree on and implement, and would present several challenges along the way. It could be 20 years before we see any sort of resolution. The good news is laws don't need to be international before they can be implemented. We should put something into place here in the U.S., and if it serves as a successful model to other countries, we could then consider expanding the idea globally.

International organizations could agree on a set of rules and regulations, similar to what has been done in the automotive industry with regard to safety and automation regulation. In order to sell cars all over the world, auto manufacturers must build a car that meets all of these requirements. The same model could apply for critical infrastructure providers, but that will also take time to develop and finalize – time we don't have in the face of today's emerging threats. Ultimately, countries developing their own set of standards in the near-term will be the best plan for defense.

All quotes in this article are attributable to Dr. Vincent Berk, CEO of network security company FlowTraq . Dr. Vincent Berk has 15 years of IT security and network management experience, and is the designer of the FlowTraq system. He is a member of the ACM, the IEEE