The Growing Issue of Cybersecurity and Resilience of the Power Grid

By Chloe Demrovsky, Executive Director, Disaster Recovery Institute International (DRI)

No one can deny that the tech revolution has impacted the nation and created the type of market innovation that stimulates economic growth. By allowing start-ups with small amounts of seed capital to challenge established giants, technology has unleashed innovation that has helped sustain the global leadership position of the United States for the last half-century. While the effect of having emerging technology accessible, the result has been overwhelmingly positive so much so that it has also created a new landscape of risks.

Technology is essential to nearly every aspect of our businesses and lives especially with growing dependence surrounding critical infrastructure. With the increased onslaught of attacks - not only from traditional hackers and hacktivists, but also from sophisticated state-sponsored attackers – there is constant risk for disruption from those seeking competitive advantage in the global economy. For a forward-thinking organization, it is a competitive advantage to bring traditional risk practices into the open with creative culture of technological innovation and to address these burgeoning problems head on.

This urgency is nowhere more essential than in the world's power grid system. The grid is not only classified as critical infrastructure in its own right, but is significant given its servicing of other critical resources, such as hospitals, emergency response facilities and transportation hubs. Maintaining a resilient power grid is essential to regional preparation, response, and recovery. Especially with the advance in the "Internet of Things" (the network of internet-connected devices), the threat to the grid is broadening and morphing making cyber resilience evermore important for all organizations - especially for those that are decidedly critical infrastructure.

Within the context of organizations, resilience is about the adaptive capacity of an organization in a complex and changing environment. It is about having the means to elicit a communication framework that enables multi-level feedback to identify systems that appear strong but with systemic vulnerabilities (think "too big to fail") and may not withstand extreme duress in the case of an incident.

Communication can break down because of proprietary systems and cultural factors. We are reminded that resilience is a mindset that combats the tendency to put up internal barriers and instead promote a culture in which all managers across the enterprise are considered risk managers, thus leading to all employees having some degree of responsibility for cybersecurity. In order to be successful, resilience has to be an organizational priority at the strategic level and be integrated into all organizational activities, which will allow for continuous improvement and a more resilient power grid system.

The threat to the world's power grid is aggravated by the continued underinvestment in infrastructure. There is a gap between private sector efforts to keep the infrastructure under their control and up to date - which is reasonably successful and upheld by the governments. However, governments have largely failed to invest in the necessary upgrades and providing state funding and other traditional initiatives. The system is already vulnerable due to this prolonged underinvestment, which prevents the necessary increase in tentative measures that are posed by today's need for cybersecurity. Some of the potential effects could include the failure of critical infrastructure, the breakdown of essential information networks, vulnerability to large-scale destructive cyberattacks and massive incidence of data fraud and data theft. Targets are pinpointed for a reason and that reason is not eliminated once a single attack has been addressed. The attacks will continue to re-occur. The world power grid will continue to be a threat because it is a high-value target.

The cybersecurity effort is ongoing and here to stay, because the cyber threat and speculative forecast is expected to increase. This will occur for the following reasons:

- ***Barriers to entry are lower, not higher:*** With it becoming easier to gain the skills to launch a cyberattack, there are more and more diverse, technically-skilled players in the game, ranging from unaffiliated wolf hackers, to nation-state actors, both of which make it increasingly difficult to monitor every point of entry. There are more attack vectors with connected industrial control systems that are becoming more evident in the connection through the "Internet of Things."
- ***Attribution:*** The inherent structural anonymity of cyberspace provides safe havens for malevolent actors making identification a complex problem. The most motivated actors (i.e. cyberterrorists) are becoming more sophisticated and gaining expertise. These actors begin to pose a real threat when they have both the technical capability and the will to use it. This is different from the nation-states, which are usually deterred from doing so because of other economic factors, interdependencies, and the threat of retaliation. Another level of complexity is added if the organization is faced with an insider threat.
- ***New tools:*** Cyber tools are being used to run both financial and physical infrastructure, which increases the fiscal interdependencies. The challenge is to preserve the net-positive of these new tools - like the "Internet of Things" and cloud-computing - and by extension of the Internet itself as a resource in the face of proliferation with these harmful tools. Information needs to be disseminated to educate the public and other actors about the threats that exist and how to prepare for them.
- It is not an IT issue. With the importance of technology at the core of business, a cyber breakdown is no longer just an issue for the tech department, but also for anyone charged with managing business risk. The scope of concern is enterprise-wide and this is especially true for all businesses, as the world power grid maintains and powers businesses and the world economy.
- Have a plan. Having a continuity plan that addresses all the complexities of cybersecurity is essential for protecting infrastructure. It is not possible to fully eliminate cyber intrusion, so it is important to have a standard action plan for what needs to occur when the system has been infiltrated and how to protect the core business once that has happened.
- ***Protect and Prepare:*** It is impossible to prevent every attack, so from a technical standpoint, it is essential that we invest not only in prevention, but also in protection and response. Organizations can recover faster once an attack has been identified if it can be quickly responded to when the breach does occur. During an incident, it is essential to communicate the problem, indicate that it is being addressed and mitigate any future risk through a plan that will prevent it from happening again.
- ***Invest in people:*** Investing in technology is good, but it is insufficient without an accompanying investment in people and processes. People need to understand how to use the technology effectively or it will not address the threat. This is an area where a lot of companies fail.
- ***Teach cyber-hygiene:*** 80% of attacks can be prevented or mitigated through good cyber-hygiene practices. Human error remains a leading entry point – click on just one of those clever phishing emails and the whole system could be at risk. So take a moment to learn how to practice cyber-hygiene by educating yourself, your family and your organization about basic online safety.

Cybersecurity has grown beyond just being a responsibility of the IT department. It is now an enterprise-wide issue with far-reaching capabilities that have segued into important phases of the government continuity planning process to withstand a potential cyber incident. Every organization's continuity program should maintain an expanded protocol to assess the risk and have an emergency preparedness plan in place to deal with potential effects of a cyber incident. Continuity professionals – no matter if part of the energy sector or another organization - are charged not with the technical aspect of cybersecurity, but rather with assessing, preparing for, and reacting to the operational effects of a cyber incident. In order to better protect organizations, a resilient program must be designed that is flexible and encompassing enough to endure if put to the test with a significant duress. The cyber threats to the world power grid pose a significant example.

In conclusion, the takeaways in managing the threat of cyberattacks can be summed up with a few reiterated points that can help to reshape our thinking about how to deal with cybersecurity in the context of protecting the world power grid:

Forbes reported recently that a study by the University of Cambridge Centre For Risk Studies showed that a major cyberattack on the U.S. electric grid could cause over $1 trillion in economic impact and roughly $71.1 billion in insurance claims. The report looks at the financial impact of a scenario in which 15 states and Washington, D.C. suffer a blackout as a result of a cyberattack on the power grid.

The cyber threat against critical infrastructure, including the world power grid, is real and growing. We are addressing a proliferation of complexity in the risk landscape. Modern threats are interconnected and multifaceted. Cyber threats are not unique to one geographical district nor one single sector or industry. This interdependency does not just exist within traditional sectorial boundaries, but reaches across them to such an extent that it would be impossible to find a solution that relies purely on the government or purely on the private sector. A hybrid approach is necessary through formal public-private partnerships, but also through informal professional networks and economic transactions. As resources for new projects are constricting as fast as the political will to drive them, existing government agencies are increasingly looking to a network-based solution involving a multitude of actors rather than a traditional hierarchical structure.