Geopolitics, Infrastructure, and Cyber: A Perfect Storm of Risk

LUKE TENERY

Cybersecurity; Incident Response; Cyber Investigations & Forensics

luke.tenery@ankura.com
+1.312.252.9514

BILL BRAY

Former Senior Intelligence Community Professional

william.bray@ankura.com
+1.202.797.1111

SCOTT CORZINE

Cybersecurity Strategy, Risk Management, & Operational Resilience

scott.corzine@ankura.com
+1.646.291.8596

Leaders today find themselves having to make important business and policy decisions in new geopolitical and technology paradigms where global socioeconomic and political battles are increasingly fought in cyberspace. In this new type of warfare, all businesses, political groups and government entities are vulnerable to becoming, at a minimum, collateral damage. Decision-makers and policy makers must account for this in both their enterprise risk management plans and policy deliberations.

While both state and non-state actors have been engaging in cyber espionage for some time, 2016 saw a tremendous increase in high-profile cases of offensive geopolitical shaping actions in cyberspace. These activities are no longer simply about stealing military or economic secrets, they are instead efforts to create advantageous or favorable economic or political conditions for these malign actors. In many cases, these cyber actors surreptitiously compromise security and emplace digital tools or malicious software for future execution at a time of their choosing. These increasingly sophisticated cyber warriors choose this method more frequently now because it is easy to hide their fingerprints, making decisive attribution and retaliation difficult or unlikely.

Whether directed against a nation's electoral process, government or military infrastructure, or private economic infrastructure, states with dedicated foreign cyber espionage and attack capabilities are becoming ever bolder in their efforts. States currently lacking the capability will

INSIGHTS

increasingly work to develop it. Furthermore, criminal enterprises as well can go beyond traditional theft and adopt these more sophisticated targeting tactics to damage infrastructure or to threaten to do so for economic gain.

The "extended enterprise" creates the increasing potential for multinational companies to become direct victims or collateral damage in the geo-cyber battlesphere as nation-states and non-state actors acquire these capabilities and shift to cyber-based operations and strategies. High value targets include energy infrastructure, electric grids, transportation systems, hospitals, process manufacturing and water supplies, placing increasing value on these organizations' vendors and third-party resources. The digital backbones for entry into these critical facilities reside on both the Internet and computer networks internal to an organization. The remediation and repair cost due to cyber intrusions, disruptions, damage, or denial of these critical services is expected to be in the billions of dollars in 2017.

The "extended enterprise" creates the increasing potential for multinational companies to become direct victims or collateral damage in the geo-cyber battlesphere as nation-states and non-state actors acquire these capabilities and shift to cyber-based operations and strategies. High value targets include energy infrastructure, electric grids, transportation systems, hospitals, process manufacturing and water supplies, placing increasing value on these organizations' vendors and third-party resources. The digital backbones for entry into these critical facilities reside on both the Internet and computer networks internal to an organization. The remediation and repair cost due to cyber intrusions, disruptions, damage, or denial of these critical services is expected to be in the billions of dollars in 2017.

A cyber-induced catastrophe that results in extensive physical destruction and human suffering would transcend a mere 'cost of doing business' calculation. Attacks on the "industrial internet of things" (IIOT) – the addressable industrial control systems that drive critical infrastructure installations – would result in potentially massive impact on public health, process safety, mission assurance, and entire regional economies. These attacks would entail a recovery measured in months or years because of damage to long lead time capital equipment. Rather than shelve these potential incidents as "black swans", leaders would be advised to examine the long term real cost of the resulting impacts, based on their risk appetite. This cost includes severe, but less obvious costs. Many insurance policies lack clear language – or specifically exclude – claims to the destruction to physical equipment from a cyber cause. The credit rating agencies are considering how to factor into rating guidance the exposure of critical infrastructure entities to this recently unimaginable type of risk – precisely because of the outsized impact largescale damage would have on operational and financial stability.

A CYBER-INDUCED CATASTROPHE THAT RESULTS IN EXTENSIVE PHYSICAL DESTRUCTION AND HUMAN SUFFERING WOULD TRANSCEND A MERE 'COST OF DOING BUSINESS' CALCULATION.

That said, it is important to note that hackers and other malign cyber actors will target any industry they can profit from in terms of political or economic gain. At the crossroads of crime and politics, underground networks of interconnected actors and nefarious syndicates use the same tactics for different ends. For example, almost all personally identifiable information (PII) offers at least some value on the Dark Web, whether for identity theft, an advanced targeted attack, or intelligence purposes. Cyber criminals often work with or for political actors to breach systems in a variety of verticals that target similar if not the same networks and systems.

INSIGHTS

Geopolitically speaking, this means there exists a large and growing number of actors with the capability and intent to penetrate unsecured networks, and that suggests a three-pronged approach to cybersecurity. Whether in the public or private sector, it is time to think more seriously and in a broader context about cyber resiliency. One way to do that is to frame a cybersecurity mission around these three pillars: **Preparation, Response, and Remediation.**

Preparation: Responsible corporate risk management plans must assume that successful attacks are inevitable, and thus include a comprehensive assessment of cyber risk that centers not just around cost, but also around physical safety and infrastructure integrity. Several cases recently in the news demonstrate the importance of developing a plan that protects private and public infrastructure. The Saudi Arabian civil aviation department was attacked in November 2016 with a malicious cyber tool that had been reused from a previous attack on a private enterprise (Aramco) four years earlier. Failure to adequately identify, inventory, and prioritize risks resulted in an expensive cyber-attack that could have easily been prevented with just a little preparation.

Response: A competent and thorough forensic analysis and incident response to a cyber intrusion or attack is critical to developing an accurate damage assessment, mitigating any continued threats, protecting evidence ahead of possible litigation, and embarking upon subsequent security improvements. But also highly important is attribution analysis. Good attribution analysis is the foundation for a more targeted and effective response. Response extends to the crisis communications that must be planned for interpreting the impact to stakeholders, regulators and the media.

Remediation: Having in place well designed and exercised operational resilience plans (for business continuity and disaster recovery) is now a baseline expectation of serious management by shareholders, markets, media and regulators. In addition to internal mitigation and incident response to the security incident, remediation efforts should include productive partnership with law enforcement and national security authorities to hold offending parties to account and deter future attacks.

If more robust protective and risk mitigation measures are not implemented, cyber threats to organizations with significant critical infrastructure presence will only increase in frequency and sophistication.

Ankura Consulting has a unique combination of geopolitical and cyber expertise to help clients better understand the nature, source and the risks of these threats, prepare for the potential of such attacks occurring, determine the nature and extent of any attack, and formulate a comprehensive response if needed.

ABOUT US

Ankura is an expert services firm defined by *HOW* we solve challenges. Whether a client is facing an immediate business challenge, trying to increase the value of their company or protect against future risks, Ankura designs, develops, and executes tailored solutions by assembling the right combination of expertise. We build on this experience with every case, client, and situation, collaborating to create innovative, customized solutions, and strategies designed for today's ever-changing business environment. This gives our clients unparalleled insight and experience across a wide range of economic, governance, and regulatory challenges. At Ankura, we know that **collaboration drives results**.