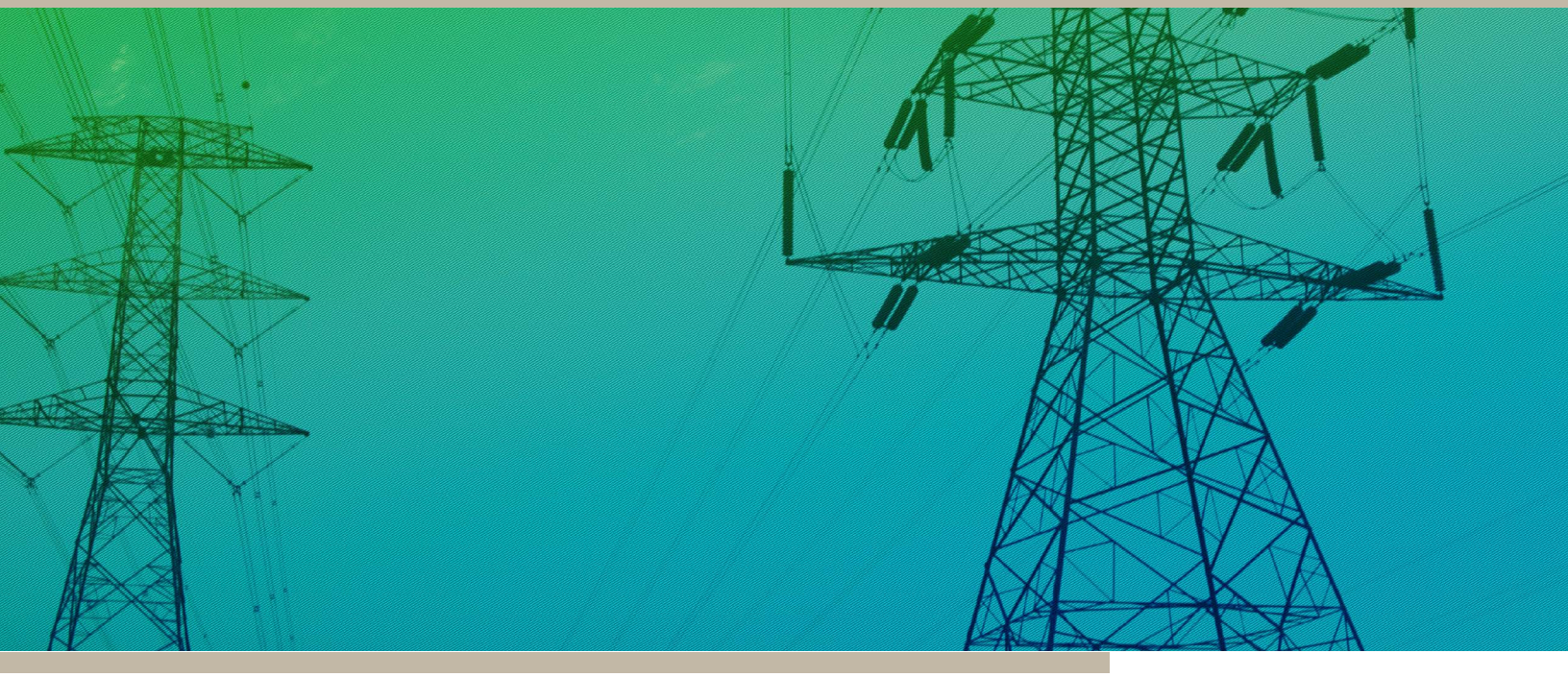
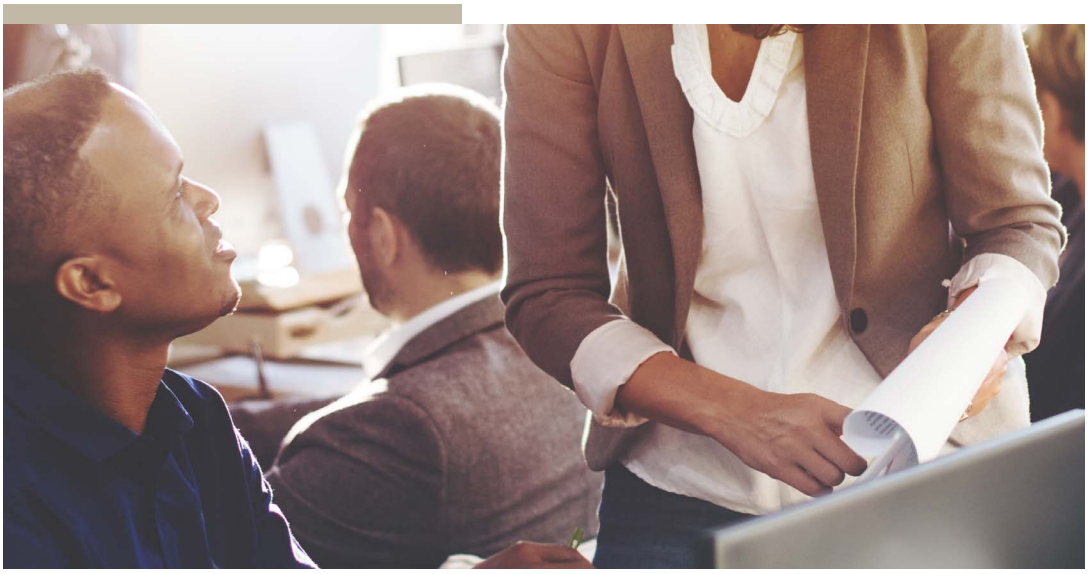


TARGETS OF OPPORTUNITY

CYBER SECURITY FOR ENERGY AND UTILITY COMPANIES

Canada's energy and utilities companies' exposure to cyber security risk continues to rise, as the country's critical infrastructure becomes an increasingly attractive target for cyber criminals. Boards and leadership teams have responded by escalating cyber security concerns to the top of the agenda. Unfortunately, companies often fail to understand both the nature of the cyber security threats they now face and the scale of the risk to their business. Without sufficient risk management and mitigation plans, boards will fail to effectively provide governance. This leaves many companies far more vulnerable to cyber attack than they realize.



A PRIME — AND UNDERPREPARED — TARGET

Energy and utility companies worldwide find themselves under constant threats for many reasons, but one in particular stands out: our world is completely dependent on the critical infrastructure they own and operate. A cyber attack that shuts down a power grid or water distribution could bring a city to a rapid halt, with significant and hazardous safety, economic, social and health consequences, possibly even including fatalities.

Customers' personal information could be stolen, leading to identify theft and a spate of fraud and financial losses. Confidential data such as business plans or acquisition targets could be taken by a rival leading to a competitive disadvantage in the market. In the aftermath of any such event, governments, businesses and citizens will pin the blame on the utilities involved.

The risk of such an attack in Canada is very real. The Canadian Security Intelligence Service (CSIS) last year warned the industry of the rising risk of cyber espionage and attacks on key infrastructure, from pipelines to storage facilities to transmission towers. The U.S. government has also expressed concerns over cyber attacks on Canadian energy and utility companies, driven in part by the interconnections of the two countries' power grids.

Such warnings and concerns are putting the Canadian energy sector cyber preparedness under more scrutiny. Understanding the complex nature of cyber security today is vital to developing an effective risk management strategy.

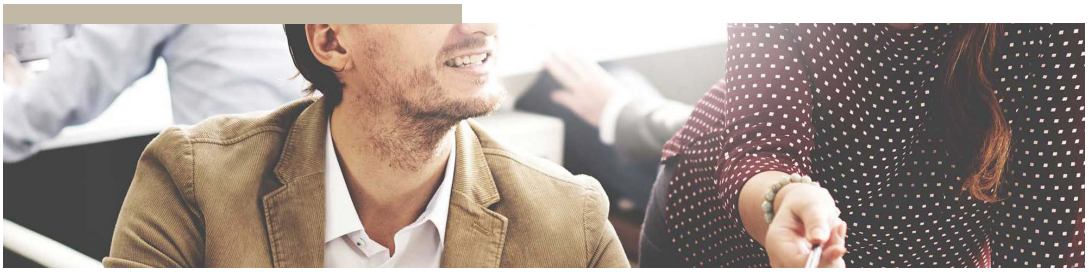
1 http://www.cbc.ca/news/business/canada-pipelines-energy-security-risks-1.3939588

CYBER RISKS ARE BUSINESS RISKS

Often, energy and utility companies address cyber risk in isolation, as if it were a special category of risk on its own. In fact, they are integrated with operational risks, yet many organizations don't examine them through a holistic risk management lens.

A data breach in which customers' personal and financial information is stolen could result in significant fines, fleeing customers and lost reputation. A lengthy outage could invoke the ire of governments, business and regulators alike, leading to penalties and the imposition of wholesale changes from above. Businesses left without power for days due to an attack could take energy and utility companies to court to recoup lost revenue, resulting in years of costly litigation.

A real-life example occurred in December 2015 after a cyber attack disabled the western Ukrainian power grid for hours, underscoring concerns about power grid vulnerabilities. Companies that fail to make this connection can soon discover their enterprise risk planning isn't as effective or comprehensive as it needs to be.



CYBER CRIMINALS: DIVERSE, SOPHISTICATED, PROFESSIONAL

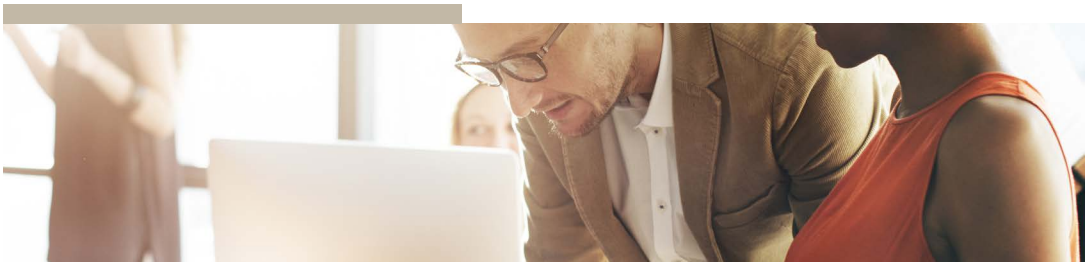
Companies' defences are under attack from a wide range of highly sophisticated organizations with diverse objectives and the resources to execute large, continuous campaigns:

- State-sponsored hackers infiltrating companies to acquire competitive intelligence, sensitive financial information or intellectual property and take systems offline to disrupt our nation's economy.
- Hacktivists breaching defences to find and disclose confidential information in an attempt to embarrass, incriminate or damage the reputation of a company.
- Organized criminals running phishing campaigns or ransomware attacks as a means to generate illicit funds.
- Terrorist groups intending to cause widespread panic by shutting down or damaging vital infrastructure such as power grids.
- Individuals trying to breach a company's defences for little more than bragging rights or to establish their reputation.
- Rogue employees or trusted third parties who have decided that they want to cause harm.

Energy and utility companies face cyber criminals who are well organized and motivated to accomplish their mission. They often communicate successes between themselves more than the companies themselves share information about attacks and breaches. The largest groups conduct themselves much like "normal" businesses. They set goals and targets, developing sophisticated strategies that are often tailor-made to breach a specific company. And they're successful: research has found that 5 of every 50 phishing emails succeed, a response rate that any marketing executive would envy.

CYBER BREACHES ARE THE RULE, NOT THE EXCEPTION

Modern companies in every industry are digitally connected in ways unimaginable only a decade ago. Power plants, transmission lines, remote monitoring equipment, vehicles, computers, employee mobile devices are connected to the internet. In the physical world, a criminal disguised as a vendor or salesperson could gain access to a company's systems while on premises or leave a host of malware-laden USB sticks behind as "gifts" for company personnel. Cyber criminals have many vectors of attack and a company's defences are only as strong as the weakest link. Criminals have to be successful once, you have to be successful all the time. Breaches are inevitable. It's a matter of when, not if. Are you prepared?



PILLARS OF CYBER SECURITY INCLUDE MORE THAN IT

At many companies, cyber security discussions swiftly become discussions about IT security. However IT security is only one aspect of a company's security program — and it's often the last one cyber attackers will try to breach.

Effective cyber security has three aspects: physical security, people security and IT security. Physical security involves making sure would-be cyber attackers can't access offices, plants, stations or other facilities and thus gain access to a company's network from the inside. People security involves ensuring managers and staff are trained in how to be security-minded and vigilant for suspicious behaviour and equally suspicious communications. And IT security entails firewalls and other digital safeguards that form the more traditional foundation of any cyber security effort.

Sophisticated hackers will usually attempt to gain access to a company's network via physical means or through the company's own people using phishing emails. Companies that want to significantly improve their overall cyber preparedness would do well to invest in improving physical security and increasing their employees' cyber security

TACKLING THE CYBER SECURITY CHALLENGE

As they face ever-greater cyber security risks, Canada's energy and utility companies need to adopt a new approach to cyber security, one that reflects today's realities, addresses business risks and responds to incidents and breaches with speed and resilience.

Sophisticated hackers will usually attempt to gain access to a company's network via physical means or through the company's own people using phishing emails. Companies that want to significantly improve their overall cyber preparedness would do well to invest in improving physical security and increasing their employees' cyber security

START BY FOCUSING ON CRITICAL BUSINESS RISKS

Any cyber security discussion should start with an assessment of the organization's major business risks and the interconnections between those risks. Without this perspective, companies could overlook something critical. A comprehensive enterprise risk assessment can uncover important risks that could harm the company's finances, operations or reputation among customers, business partners, the finance community, government, regulators or the wider public. Identifying key business risks better enables companies to determine which assets and systems need to be protected and where to focus their security investments.

ASSESS CYBER SECURITY MATURITY

Companies should undertake an assessment of the relative maturity of their overall cyber preparedness and the existing security controls that protect important business assets. The assessment should review of their overall security controls, key business areas and known threat agents. This maturity assessment provides companies with a prioritized risk reduction strategy; a road map that will help focus both budget and resources in the areas of higher risk first.

Once a baseline is established, annual reviews should be done to assess progress and re-evaluate the company against evolving threats, industry standards and best practices.

SECURITY RED TEAM EXERCISES

Red team exercises should be carried out to uncover vulnerabilities in companies' networks, applications and systems. An external advisor can be engaged to review and test existing process and technology controls to gauge their strength and ensure they're functioning as intended. These exercises go beyond typical penetration testing of this network or that application and enable companies to experience the closest thing to a real cyber attack, revealing the strength or weakness of physical, people and cyber security measures as well as the effectiveness of any response and communications plans.

PRIORITIZE CYBER SECURITY EFFORTS

After assessing their business risks, determining the overall maturity of their cyber preparedness and identifying vulnerabilities, companies can develop short-term and long-term plans to invest in the improvements needed to close lower any risks that are beyond their risk tolerance. Companies should focus on protecting their most important assets, systems and data first, including private personal information about employees and customers and financial information.

By focusing on the highest priority business risks first, companies can ensure they get the biggest impact from their limited security investments. In future months and years, companies can move "down the list" to address subsequent priorities.

DEVELOP A CYBER RESILIENCE PLAN

A cyber resilience plan provides organizations with a clear framework for handling inevitable cyber breach incidents. It sets out exactly what needs to happen in response to an incident to stop the breach and limit the damage to the company and other affected parties. Typically, they also involve post-incident analysis so that the company can identify how to improve its cyber preparedness moving forward.

The communication plan is an important part of any cyber resilience plan. When a breach occurs, it's absolutely essential that people understand who needs to be contacted, when and what they need to be told. Energy and utility companies may need to inform executives, directors, customers and suppliers and shareholders, not to mention regulators, government ministries, law enforcement or emergency services. Open, clear and accurate communication is key; companies can prepare many messages in advance, filling in the relevant details during the crisis.

Organizations should practice their cyber resilience plans just like they practice health and safety drills and disaster recovery or business continuity plans. This will reduce the risk of confusion and poor decision making in the heat of the moment.

CYBER PREPAREDNESS

Canada's energy and utility companies face a world where they are under constant threat of attack. Careful preparation can help ensure they protect the most essential parts of their business and respond rapidly and effectively to incidents.

With one of Canada's largest cyber security advisory practices, MNP is well-positioned to help you develop a cyber security strategy that addresses your unique situation, risks and objectives. Leveraging our extensive multi-industry experience and proven methodologies, we deliver practical, scalable cyber security solutions and actionable advice.

For more information on how MNP can help, contact:

Jason Hails
National Leader, Energy and Utilities
T: 1.877.251.2922
E: jason.hails@mnp.ca

Danny Timmins
National Leader, Cyber Security
T: 905.607.9777 x 230
E: danny.timmins@mnp.ca

Richard Arthurs
National Leader, Governance and Risk Management
T: 1.877.500.0792
E: richard.arthurs@mnp.ca

ABOUT MNP

MNP is a leading national accounting, tax and business consulting firm in Canada. We proudly serve and respond to the needs of our clients in the public, private and not-for-profit sectors. Through partner-led engagements, we provide a collaborative, cost-effective approach to doing business and personalized strategies to help organizations succeed across the country and around the world.

AON
BESTEMPLOYER
PLATINUM | CANADA

Visit us at MNP.ca

Praxity
MEMBER
GLOBAL ALLIANCE OF INDEPENDENT FIRMS