Beneath the surface: phishing and other cyber risks for energy firms

How internal and external actors can compromise cyber security

Empower Results®

How are cyber risks changing for energy firms?

Although energy companies' risk profiles have historically focused on supply, resources are plentiful and contingency plans have helped to manage this particular risk. As risk managers turn their attention to the integrity of their cyber security, rapidly evolving cyber risks are creating unknown exposures.

An increasing reliance on digital processes are exposing energy firms to changing cyber risks. While many energy firms have robust risk management strategies in place, the accelerated changes in cyber capabilities and processes are creating gaps and exposures; risks which can remain unknown and unaddressed until it's too late.

Experts at Aon's 2020 Energy Risk Symposium identified key challenges for energy firms:

1. A general lack of awareness and training of cyber security
2. Agile working behaviours (working remotely, connecting to unsecure networks, vulnerabilities of standard products and mobile devices)
3. Extrapolated risks from supply chains
4. Insufficient separation of data networks
5. Ageing controls
6. Lack of physical security
7. Targeted attacks including phishing and ransomware
8. The importance of incident response

Energy firms' complex and interconnected digital systems are vulnerable to both accidental damage from internal failings and intentional damage from criminals and hostile governments.

Deep waters: phishing and ransomware

According to experts, approximately 90% of phishing emails contain ransomware. Often a multi-stage process involving a number of attackers, ransomware moves interactively through a firm's digital environment and encrypts files, even targeting back-up files to block recovery efforts. Ransoms for lost data typically exceed USD 1 million, but many cases have exceeded USD 10 million.

While traditional phishing incidents such as 'credential harvesting' remain simple but effective, ransomware risks are changing rapidly. Assumptions of the identity of ransomware attackers often conjure an image of a hidden figure in a basement, but the reality is that attackers are often professionals running a highly sophisticated operation, sometimes even often offering call centre support.

Trending: hotel hackers

Travelling business executives working remotely in hotels worldwide are potentially exposing firms to ransomware attacks. A typical attack often begins with the target checking into a compromised hotel and then logging into the Wi-Fi, where they are prompted to enter their surname and room number. The attackers then offer an update for legitimate software, and their 'welcome packages' act as installers for a backdoor, allowing the intruder to use data collection and hunt for cached passwords.

An increased reliance on data assets for business results increases the severity if the impact on the business if those assets are compromised.

Control and prepare: managing cyber risks

"No industry is immune from cyber-attacks. The most important things that energy executives can do is implement proactive cybersecurity measures such as risk assessments, penetration testing and employee training while also having a robust incident response plan."
Heather Hughes, Aon

Control what you can and prepare for what you can't. Working with an external partner with consulting capabilities can help firms stress test their defenses and identify any vulnerabilities in their security measures. With a clear understanding of their security posture, energy firms are able to make informed decisions about risk management, including whether to retain or transfer risk, and how to access suitable coverage.

Given that phishing and ransomware attacks are becoming increasingly sophisticated, investing in staff training is critical. Although individual actions are autonomous, providing staff with education and guidance is an important way to manage internal threats to cyber security.

Deploying an incident response team is a key way to manage an incident. An effective incident response team includes multiple representatives from external counsel, forensic experts, crisis communicators, notification firms, insurance agents and law enforcements.

Breach responders are also a key component of an incident response team. Establishing a professional relationship with a breach responder helps energy firms build trust with their professional partners, and limit any damage sustained by an incident by acting with efficiency. Breach responders may operate on a retainer or fixed fee basis to suit different circumstances and needs.

If you would like to discuss any of the issues raised in this article, please contact your local expert.

Contact Information

Heather Hughes
Vice President, Engagement Management, Stroz Friedberg – An Aon Company
+1 832.459.6790
heather.hughes@strozfriedberg.com

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.