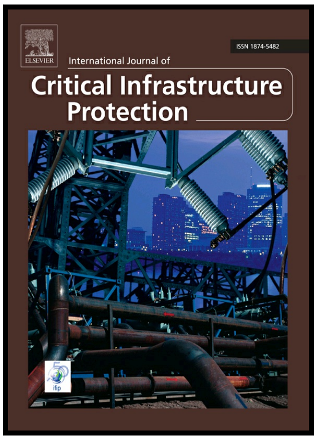

www.elsevier.com/locate/ijcip

Cyber security trends: What should keep CEOs awake at night

Richard Piggin

PII: S1874-5482(16)30013-0
DOI: http://dx.doi.org/10.1016/j.ijcip.2016.02.001
Reference: IJCIP183

To appear in: *International Journal of Critical Infrastructure Protection*

Cite this article as: Richard Piggin, Cyber security trends: What should kee CEOs awake at night, *International Journal of Critical Infrastructure Protectior* http://dx.doi.org/10.1016/j.ijcip.2016.02.001

Cyber security trends: What should keep CEOs awake at night

Richard Piggin, Atkins, Woodcote Grove, Ashley Road, Epsom, Surrey, United Kingdom KT18 5BW

Recent publications by the U.S. Department of Homeland Security and several industry entities report significant increases in the number of cyber attacks against industrial control systems. The sophistication of attacks is also increasing as is the likelihood that they will be physically destructive and cause significant loss. Recent breaches demonstrate that perpetrators have been implanting malware in control system software and repurposing industrial software and protocols to conduct system reconnaissance. Research has also shown that attacks are increasing in severity with the greatest damage to corporate reputation and branding. A correlation between reputation damage and share price has also been observed. Unfortunately, senior corporate executives are generally unaware of the current threats, system vulnerabilities and the potential business impact and legal exposure.

On December 23, 2015, the Ukrainian media reported that a cyber attack had left half the homes and 1.4 million people in the Ivano-Frankivsk region without electricity. Services were restored within a few hours, but this was largely done by manual intervention instead of sanitizing and then using the (compromised) automation systems. The Slovakian security firm ESET announced that the incident was not isolated and that multiple electricity companies had been affected simultaneously. Reuters reported that similar malware was found in IT networks at Kiev's Boryspil Airport, including a network used for air traffic control. Ukraine blamed Russia for the incidents.

The U.S. Industrial Control Systems Computer Emergency Response Team (ICS-CERT) working with Ukraine's CERT-UA confirmed the presence of Black Energy 3 malware. The ICS-CERT alert is yet another warning about a sophisticated malware campaign that has targeted industrial control systems dating back to 2011. Black Energy 2 (from 2014) leveraged vulnerabilities in industrial control systems that were directly connected to the Internet to deliver malware – it had reconnaissance functionality, but no destructive modules. In contrast, the new Black Energy 3 variant appears to have been launched using a spear phishing campaign with malicious Microsoft Office (MS Word) attachments. An additional round of spear phishing attacks in January 2016 used a malicious Microsoft Excel macro, purporting to require a newer version Microsoft Office to thwart security.

The Black Energy 3 incursion is one of a few confirmed attacks against the electric power grid, although no direct causal link has been established between the malware and the Ukrainian power outage. However, other attacks against industrial systems have caused physical harm. These include Stuxnet that targeted the Iranian nuclear program in 2010 and a 2014 attack that caused "massive" damage to a German steel mill.

By comparison, the Havex malware of 2013 and 2014 targeted energy sector control systems using multiple infection routes, including spear phishing, infected control system software downloads from legitimate websites and compromised industry websites. The malware was used for intelligence gathering – enumerating operational technology