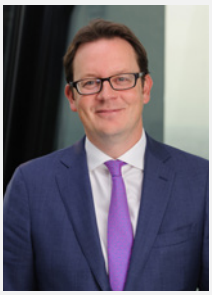
a window into cyber



a note from Ben Maidment

BRIT

Cyber crime may seem like a fairly recent phenomenon, but hackers have been playing havoc with key pieces of infrastructure for decades. This month, Éireann Leverett guides us through a history of attacks on industrial control systems and the chaos they can cause.

As industry becomes increasingly digitised and smart technology is built into even the most innocuous pieces of equipment, the potential for cyber crime increases.

At Brit, our emphasis is on helping businesses put in place sensible systems and protocols to avoid these attacks, educating teams so that the stories remain as past cautionary tales rather than headline news.

this month's author: Éireann Leverett

Co-Founder, Concinnity Risks
Co-Author, 'Solving Cyber Risk'

Éireann works in various research departments and loves quantifying cyber risks and studying cyber crime. He co-chairs the Cyber Insurance Special Interest Group at FIRST.org, and speaks publicly at both hacker and insurance conferences regularly. He likes writing essays and exploits, and sitting in the gardens and libraries of Cambridge learning.

BRIT

from Maroochy Shire to EKANS

a brief history of cyber-attacks on industrial control systems

by Éireann Leverett | Read time: 4 minutes

When I was younger, stories of the river catching fire due to industrial pollution were common. So common, in fact, I sit on the porch at my mother's house most summers drinking a beer called Burning River Pale Ale. I know, it sounds like a common and charming tendency towards exaggeration, but the Cuyahoga river caught fire at least 13 times. There wasn't even any hacking involved!

So what happens to industrial systems when they get hacked?

Well, there's Maroochy Shire where 800,000 gallons of sewage were released into parks, rivers, streams, and even a hotel lobby back in '99. Vitek Boden hacked radio controllers at substations around the area with a laptop from his car. He got away with it on 42 occasions before an engineer could convince his management they weren't just glitches.

In 2003, a nuclear power point called Davis Besse was infected with Slammer worm. That worm wasn't even written to affect industrial systems, but it disabled a safety parameter display for 5 hours. In 2006, some hackers took control of servers at a water facility in Harrisburg, repurposing the servers to be used for gaming. We're lucky they just wanted to play games, and they weren't much different than a teenage boy in Poland whose interest in electronics got slightly out of hand. The City of Lodz's transport team was forced to launch long investigations after trams crashed and people were injured in 2008. They eventually tracked down the teenager on CCTV footage, who was using a modified universal remote control to send infrared signals to the track controls.

In 2003, a nuclear power point called Davis Besse was infected with Slammer worm. That worm wasn't even written to affect industrial systems, but it disabled a safety parameter display for 5 hours.

There are many more of these minor incidents, but things got really interesting in 2010 when Stuxnet was discovered. It's a bigger story than we can tell here, and I'm sure you've already heard parts of the tale. The point is that nation state backed hackers began aiming at each other's infrastructure. Their motive might have been anti-proliferation of nuclear material, but they started a proliferation of cyber operations we still struggle with to this day. From the Dragonfly operations against various critical infrastructure sectors, to the power outages caused by hacking in Ukraine.

Today even ransomware gangs are getting in on the action, from Maersk to Norsk Hydro, once these systems were shown to be penetrable...it wasn't just the stuff of spies anymore. When Industroyer was found targeting safety systems, things had moved up a level. There's even a new strain of ransomware called EKANS that is building functions into the malicious code to map out and stop industrial system software.

Casandra knows, we get tired of predicting such things!

"Databases of vulnerable critical national infrastructure will be traded in the future like the data of stolen credit card numbers today."

I have vintage champagne that didn't age as well as those words I wrote almost a decade ago. I still remember those burning rivers and how they motivated me to make the world a safer place. All of this may seem incredible, but don't take my word for it. You are probably in just the right place while reading this to fire up a search engine and find out for yourself. Besides, my champagne is getting warm, and it's a lovely summer evening.

BRIT

physical education:

cyber risks in oil & gas

James Bright ACII, Senior Underwriter, War and Terrorism | Read time: 6 minutes

Cyber threats are not just limited to the digital world and they can manifest themselves as direct risks to physical assets – especially in the vulnerable oil and gas sector.

Discover what the rapid rise of cyber-attacks means for sectors with an unprecedented reliance on operational technology. It's time the industry was educated on how we can better adapt and help in a post COVID-19 world.

click to read full article on PrivSec Report

from our innovation team

mitigating the cyber risks of IoT

and finding solutions

Andrea Gaglione, Technology Lead, Brit Insurance | Read time: 5 minutes

The last decade has seen unprecedented development of the Internet of Things (IoT) landscape, enabled by new distributed network technologies. McKinsey estimates that by 2025, the world will own 50 billion networked devices, contributing US$11 trillion (€10 trillion) to economies.

While this proliferation of IoT has created exciting opportunities for businesses, governments and individual consumers, it has created new risks which require mitigation. And with such rapid development and implementation of IoT technologies, it's important that individuals and organisations learn how to best protect themselves against potential threats.

click to read full article on IoT Now

highlights from Datasafe

BRIT

Datasafe is a free resource for all policyholders, which enables them to train their organisations to prevent cyber crime.

This month's focus is on Remote Desktop Protocol – a Microsoft protocol allowing remote access from one machine to another. With the rapidly growing work-from-home workforce, organizations are granting employees access to their work computers from home. Unfortunately, criminals are exploiting this explosion in remote access to infiltrate organizations and deploy dangerous malware, like ransomware, into companies with poor RDP practices.

TIPS:
How do you secure RDP?

- If you are not using RDP, disable it so no one can use it!
- Use long, complex passwords to secure all RDP logins.
- Protect RDP with two-factor authentication.
- Consider using a Remote Desktop Gateway.

Datasafe users can visit the website and download the step-by-step instructions on how to implement the above best practices from the NEW comprehensive "Securing RDP" guide.

top resources accessed:

- Cybersecurity Fitness Check
- Coronavirus Cyber Hygiene Poster
- The Year to Avoid Being Phished
- Email Policy
- Information Security Incident Response Plan

top training courses completed:

- Phishing
- Spear-Phishing
- Malware
- Password Best Practices
- Public Wi-Fi