KOVRR
Predictive Cyber Risk Modeling

How Industrial IoT Could Trigger the Next Cyber Catastrophe

Analyzing the Effect of URGENT/11 on the US Manufacturing Industry Reveals $7 Billion Exposure

AUGUST 2019

BY SHALOM BUBLIL & AMIR KESSLER

KOVRR
Predictive Cyber Risk Modeling

HOW INDUSTRIAL IOT COULD TRIGGER THE NEXT CYBER CATASTROPHE

Analyzing the Effect of URGENT/11 on the US Manufacturing Industry Reveals $7 Billion Exposure

By Shalom Bublil & Amir Kessler

Introduction

On 29th July 2019, the cyber security firm Armis announced that it had found eleven different vulnerabilities in the operating system 'VXworks' which they believe exposed around 200 million critical devices.

The team at Armis dubbed this group of vulnerabilities: URGENT/11. This report explores how the discovery of URGENT/11 demonstrates the susceptibility of global manufacturing businesses to large losses from a cyber-attack event and the potential impact on commercial P&C (re)insurers.

The Operating System at the Heart of the Issue

VxWorks is a widely used, but lesser known, lightweight IoT real-time operating system (RTOS). This operating system is embedded in over 2 billion devices in the US and worldwide.

These range from large-scale industrial machinery controlling installations such as nuclear power stations and oil production platforms, to smaller systems throughout the world's automotive, aviation, agri-business, textile, logistics and pharmaceutical facilities.

A malicious attack could affect what is known as the Supervisory Control and Data Acquisition (SCADA), the system that allows industrial organizations to gather and monitor real-time data in their manufacturing and distribution systems. Critically, VxWorks is also part of what are known as Industrial Control Systems (ICS) - software that manages the industrial processes themselves.

In simple terms, a successful attack on a SCADA or ICS has the potential to disrupt or even destroy a wide range of business-critical installations.

Not a Quick Fix

As with any type of software vulnerability, affected organizations need to patch vulnerabilities quickly.

However, in the case of URGENT/11, the necessary patches can be very expensive to apply immediately, because the affected devices are critical to day-to-day operations. Patching a vulnerability requires stopping or interrupting the device, which could lead to significant business disruption.

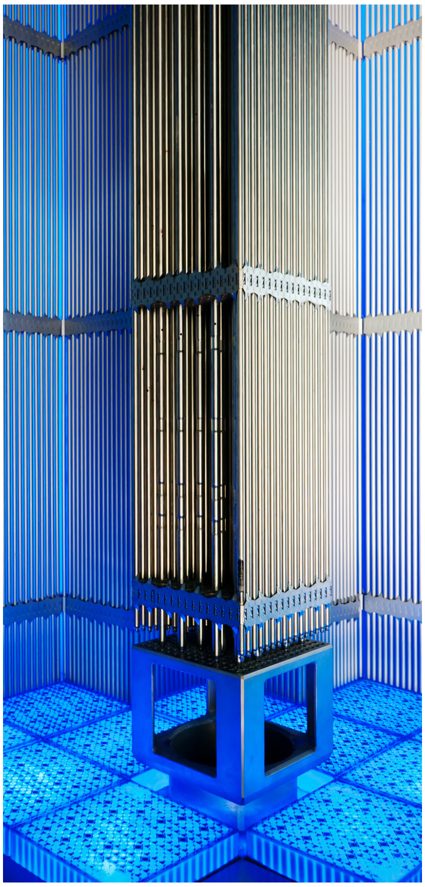
Furthermore, while very large organisations have the financial and technical resources to implement system patches quickly, smaller manufacturers - who may nevertheless be critical to the supply chain - often do not. They may buy equipment that happens to contain VxWorks, but do not expect to have to maintain the software or even be aware of its existence.

Quantifying URGENT/11's Potential Loss Scenarios for the US Manufacturing Industry

To understand the extent of companies that were vulnerable to URGENT/11, their susceptibility to being attacked, and the effect an attack might have industry wide, Kovrr deployed its proprietary technologies.

The first step was to gather real-time information about the distribution of VxWorks in the US manufacturing sector. To achieve this Kovrr leveraged its ability to continuously collect relevant business intelligence, cyber threat intelligence, external and internal security data.

As a result, we were able to identify companies with devices that were utilizing the VxWorks operating system. For internal mapping, access to multiple security vendors' data is essential because each vendor has its own expertise and distribution, in terms of geolocation, served industries, defense level focus, mapped devices, etc. In the case below involving an industrial sector, unique data focused on IoT devices is needed.



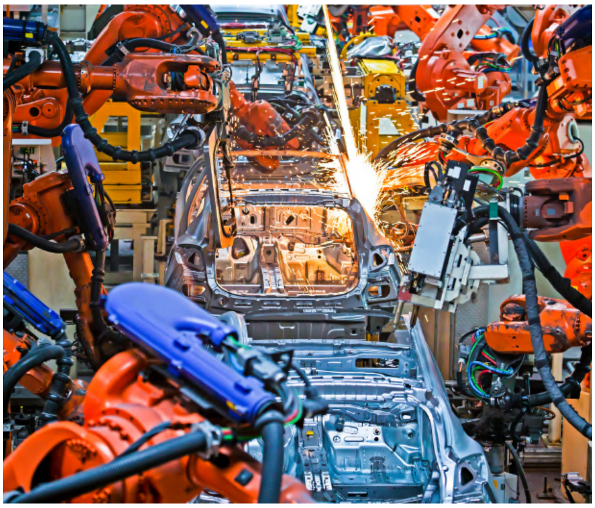
Kovrr partners with diverse types of data providers to detect and map beyond the firewall devices and security control mechanisms. By having access to Armis' proprietary IoT fingerprinting technology, we were able to produce a highly granular map of any IoT device being used by one organization.

We can then accurately assess any IoT related emerging vulnerability on clients' portfolios. In order to understand the nature of these businesses, including their sector, size and place in the supply chain; we use publicly available information linked to a variety of proprietary data-sources including our own.

This technique is similar in principle to the exposure-data cleansing and augmentation used by catastrophe modellers. Having developed a sophisticated view of the affected businesses, we have selected a series of events from Kovrr's stochastic event-set to run a series of deterministic loss scenarios.

The output of the first step identified a subset of companies utilizing the VxWorks operating system out of more than 250,000 manufacturing companies operating in the US. The results pinpointed the specific vulnerable devices, that had the largest potential exposure for critical business manufacturing operations and that are exposed to the outside internet network.

The second step ran all potential events related to VxWorks devices to generate URGENT/11's exposure data. Based on the acquired exposure data, we calculated the economic loss by utilizing company information (ex. profit, total asset value) and multiplying it by the potential impact, using a specific damage function. We were able to identify specific businesses that were affected by an attack leading to business interruption derived from the VxWorks vulnerability.



Example One: A Global Car Manufacturer in the US

A hacktivist group could use the URGENT/11 vulnerabilities to initiate a sabotage attack as an awareness campaign on the environmental impact of manufacturing internal combustion cars.

Their attack halts the manufacturing process and causes an escalating denial of service to business operations. The attack starts with partial business interruption until reaching a complete manufacturing shutdown.

Attack Initiated	Component manufacturing slowdown	Sub-Assembly Malfunction	Attack Blocked
DAY 1	DAY 3	DAY 10	DAYS 11-20
Cybercrime group launches Denial of Service(DoS) attack targeting assembly line of the leading car manufacturer in North America	A slowdown of industrial control Systems (ICS) and no immediate alerts to operators for issues with tools for remote diagnosis and repair.	Assembly line shutdown leading to inability to produce goods on time.	Incident response team able to implement network filtering to block further DOS attack exploiting the vulnerabilities.

Example Two: Multiple Small to Midsize Companies in the US Manufacturing Sector

A malicious attack exploiting URGENT/11 vulnerabilities, causes a widespread ransomware attack impacting 700 US manufacturers causing a 14-day disruption to their industrial controllers, leading to failure with environmental control sensors causing partial business interruption.

DAY 1	DAY 2	DAY 3	DAY 6	DAYS 9- 12	DAY 14
200 Manufacturers affected	700 Manufacturers affected	Forensic experts begin the investigation of the attack source	Working on POC to solve the potential source of the attack	The attack continues while the incident response team attempts to decrease the impact	Implement prevention on the network level to prevent the continuation of the attack

Calculating Potential Financial Exposures

Economic Loss - Ground Up Loss

Global car manufacturer	700 smaller manufacturers
$7,295,000,000	**$18,700,000,000**

The economic loss represents the full financial damage that the industry or the company will suffer. This number represents the entire cost of an event and does not take into account any insurance limits or conditions.

Insured Loss

Large Loss	700 smaller manufacturers
$7,295,000,000	**$13,000,000,000**

Once the economic loss is determined, the insured loss represents the subset of companies covered by relevant policies. In the case of the single manufacturer, the insured loss equals the economic loss because we assume that the company has sufficient insurance coverage.

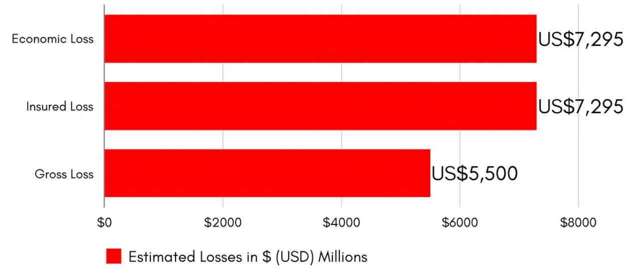
Gross Loss

Gross Loss for Automotive Co.	Gross Loss for Industry
$5,500,000,000	**$7,800,000,000**

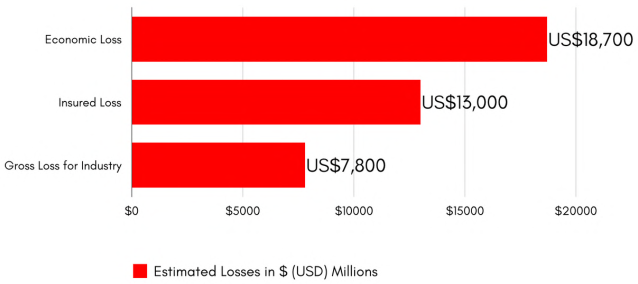
In the industry wide example, the insured loss is lower than the economic loss because the industry is composed of different sizes of businesses that use a variety of insurances. We calculated the insured loss by estimating the number of businesses that hold cyber insurance and the number of businesses that hold insurance that unintentionally covers events triggered by cyber risk (either by having no exclusion, or an exclusion that will not cover our example scenario).

In order to calculate the gross loss, we took into account terms and conditions and average waiting periods before business interruption coverage is activated. Due to the fact that no concrete conditions and limits exist in the theoretical example, the ratio between the gross loss and the insured loss is calculated using statistical data of gross and insured losses from a large data set of treaties from around the world.

Large Loss



Industry Wide CAT event



Conclusion

The vulnerabilities found in VxWorks are a clear example of how a single point of failure, such as a common operating system, can lead to a large loss or systemic cyber catastrophe.

In this rapidly changing risk landscape, risk and exposure managers must be equipped with the capability to predict and price new emerging cyber risks on-demand, both for affirmative and silent cyber risks.

In order to avoid being overly exposed, (re)insurers must have the ability to quickly determine a portfolio's exposure to newly introduced vulnerabilities.

By being able to conduct an accurate and timely delta analysis, (re)insurers can quantify any significant variance caused by the newly introduced exposure and react accordingly.

About Kovrr

Kovrr's predictive cyber risk modeling platform enables (re)insurers to transparently predict and price single, accumulated & catastrophic cyber risk.

Kovrr works with the world's leading (re)insurers; delivering underwriting, exposure, and risk management professionals unparalleled visibility into their affirmative and silent cyber risk exposure.

The Authors

Shalom Bublil is one of Kovrr's co-founders and their Chief Risk Officer.

Amir Kessler is a cyber risk modeling product lead at Kovrr

Kovrr's David Clouston, Amir Amitai, Yakir Golan, Naomi Weisz, Tom Boltman and Joseph Wolf also contributed to this report.

To Learn more please contact the Kovrr Team:
contact@kovrr.com