Humphrey Program 2025 – Cyber Simulation Overview

The Simulation:

This simulation will place participants on teams. Those teams will respond to an evolving cyber incident facing a global technology company's Costa Rican semiconductor manufacturing facility and must work together with one another to develop realistic, actionable recommendations for private companies, policymakers, and the public. The incident 'takes place' over three days, beginning with May 21, 2025. Each round will explore a different phase of cybersecurity incident response, leadership, and strategic communication.

The Incident

The scenario deals with a fictional cyber incident affecting a Costa Rican semiconductor plant. Based on documents created by Duke University, teams will manage the cyber incident as it evolves. Participants will analyze the incident, share threat information with other organizations, coordinate public and international communications, and develop short- and long-term recommendations to mitigate risk and ensure operational and strategic resilience.

The Task Force

Participants are organized into task force teams. There will be multiple of these teams, each participating in the simulation at the same time. It is important that teams play in character and keep in mind that not every piece of evidence is available. Each task force team has multiple roles:

- Chief Information Officer
- Chief Information Security Officer
- Chief Privacy Officer (Data Protection Officer)
- Director of Strategic Communications
- General Counsel

Teams are pre-assigned and listed around the auditorium, along with room assignments. Each team member will pick their role on the team. Each task force team will also have experts from the Cybersecurity Leadership Program in their room.

The Structure

Participants will work in teams to assess new developments, make decisions, and report to a simulated senior audience. The simulation evolves through documents distributed in each round, which will provide new information and create new

challenges to which teams must respond. These documents do not cover every possible implication of the scenario. The documents may also be contradictory, present unclear information, or be "discovered" out of order as often happens in cybersecurity incident response. Use the documents as a guide on where to focus.

Teams are encouraged to be creative in designing solutions to the problem. They will present their recommendations each round to the fictitious CEO of the company. Facilitators will guide discussions and act as simulation controllers. Key team deliverables will be asked for on the day of the simulation. At the end of the simulation, each team will be asked to report out to the entire group about your team's process - what worked and what do you think could work better in the future.

Simulation Schedule

ROUND 1 (Documents received beforehand)

- 13:30 - 14:15: Round 1 Tasks
- 14:15 - 14:25: CEO Brief
- BREAK until 14:40: use this time to read round 2 documents

ROUND 2

- 14:40 - 15:25: Round 2 Tasks
- 15:25 - 15:35: CEO Brief
- BREAK until 15:50: use this time to read round 3 documents

ROUND 3

- 15:50 - 16:35: Round 3 Tasks
- 16:35 - 16:45: CEO Brief

DEBRIEF

- 16:45 - 17:15

Format for Briefing the CEO

- You have up to 5 minutes to present to the CEO of Grupo Rojas
- What does the CEO need to know about the situation?

Format for Briefing the Group Post-Simulation

You have done the substantive work and the report out to the CEO. Now, report back to the entire group about your process to attack the simulation. What went well? What do you think could work better in the future? You have 5 minutes to present to the group about your team. Designate a spokesperson before you return to Sanford 04 to debrief.

Team Roles

Within each team, someone should play the role of each of the following within Grupo Rojas:

- Chief Information Officer
- Chief Information Security Officer
- Chief Privacy Officer (Data Protection Officer)
- Director of Strategic Communications
- General Counsel

More guidance will be provided for each role on the day of the simulation. Your group decides who plays who.

Facilitators

Each room will include a facilitator. Facilitators support learning, prompt key questions, ensure clarity of the scenario, and guide teams as they develop their presentations. Facilitators do not lead teams or provide answers, but they may challenge reasoning and request clarification. Facilitators are not there to fill in the blanks substantively, but to guide the conversation.

Round 1 Material

Humphrey Program

Team Roles – Grupo Rojas Cybersecurity Simulation

Below are the team roles for the cybersecurity incident simulation involving the Grupo Rojas Semiconductor Plant. Each role represents a critical function in the organization's response to the incident and will contribute unique perspectives and decisions to guide the company through the crisis.

Chief Information Officer (CIO)

- **Role -** the senior leader responsible for the management, implementation, and usability of information and computer technologies.
- **Simulation Objective** – optimize for business continuity and budget feasibility.

Chief Information Security Officer (CISO)

- **Role** – the senior leader responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected
- **Simulation Objective** – mitigate risks from cybersecurity attacks and respond quickly to cybersecurity incidents

Chief Privacy Officer (Data Protection Officer)

- **Role** – the senior leader responsible to protect against improper collection, use and transfer of personal data.
- **Simulation Objective** – mitigate risks to the theft or misuse of personal data

Director of Strategic Communications

- **Role** – the senior leader who develops and coordinates the organization's external communications both proactively and in response to incidents
- **Simulation Objective** – optimize for positive views of the organization among external stakeholders

General Counsel

- **Role** – the senior leader who oversees all legal issues for the company including risk of litigation and regulatory enforcement
- **Simulation Objective** – minimize the risk of regulatory investigations and lawsuits

Report of Cybersecurity Incident at Grupo Rojas Semiconductor Plant by Cybersecurity Firm Cirrus Cloud Solutions

Prepared for: Grupo Rojas Semiconductor Plant

By: Cirrus Cloud Solutions

[CONFIDENTIAL]

May 21, 2025, 11:48 PM

This report details the findings of Cirrus Cloud Solutions' investigation into an ongoing cybersecurity incident at the client organization — Grupo Rojas Semiconductor Plant, a critical infrastructure facility located in San José, Costa Rica. Our team was engaged to assess the scope of the incident, identify potential impacts, and analyze potential consequences.

Key Takeaways: A vulnerability in cooling software made by Cool in the Summer Software—for which a patch was issued hours earlier—was exploited to access the plant's systems. The attacker disrupted cooling operations and also gained access to personal data on employees and plant manufacturing operations. There are many unknowns about the rest of the incident and what other systems might be impacted. The responsible party is unidentified.

Technical Analysis: Our investigation identified evidence of unauthorized access to the plant's cooling systems. The attacker appears to have exploited a known vulnerability:

- **Unpatched Industrial Control Systems (ICS) software:** Legacy ICS software often lacks robust security features and may not receive timely security patches, leaving it susceptible to attacks. An initial analysis shows that the plant's cooling software had not been patched to fix a vulnerability reported by the vendor, Cool in the Summer Software, earlier in the day before the incident's impact was visible.

There are many unknowns about the attack. Other, possible factors could include: what about insiders?

- **Misconfigured Remote Desktop Protocol (RDP) access:** Inappropriate RDP configurations, such a weak password or allowing access from the internet, can provide attackers with a remote foothold into the network.
- **Supply chain vulnerabilities:** Compromised third-party software or hardware in the plant systems could introduce vulnerabilities that attackers can exploit to gain access.

The attackers may have then leveraged these initial access points to attempt further compromise. There are open questions about whether the hackers used:

what about insider with privileged credentials?

- **Lateral movement:** Once inside the network, attackers may use various tools and techniques to move laterally across the system, seeking access to privileged accounts and critical systems.
- **Privilege escalation:** Attackers may exploit vulnerabilities or misconfigurations to elevate their privileges within the system, granting them greater control and access to sensitive data or systems.
- **Data exfiltration:** If successful, attackers may attempt to exfiltrate sensitive data from the compromised systems, such as proprietary information, intellectual property, or personally identifiable information (PII).

Impact Assessment: Our initial analysis indicates that the attackers were able to:

- Disrupt cooling systems at the plant and therefore disrupt plant operations.
- Access personal data in an employee/human resources database and access manufacturing system-level data logs about plant operations.

Action Items:

- The plant's cybersecurity team and Cirrus Cloud should investigate the incident's full scope and its impacts on the plant's operations, data, systems, and customers.
- The plant's leadership should estimate the amount of time needed to get systems back up and running — and the feasibility and economic costs of just replacing systems.
- The plant's technology procurement team should contact Cool in the Summer Software and request more information about the incident and other known exploits.

MEMO: Grupo Rojas Semiconductor Plant Disruption
FOR: CSIRT-CR, Internal;
Grupo Rojas; Cool in the Summer Software
DATE: May 22, 2025
—

Internal reports from Grupo Rojas Semiconductor Plant indicate a serious and ongoing disruption to plant operations due to a cyber attack disrupting its cooling systems. The plant is an important economic and technological component of Costa Rica's innovation sector and in supplying semiconductors to Latin America and other parts of the world, especially as companies diversify supplies beyond Asia.

The CSIRT-CR is seeking information from the Grupo Rojas Semiconductor Plant; the plant's cybersecurity providers; and the supplier of the cooling system technology, Cool in the Summer Software Ltd., about:

- The exact scope of the cyber incident and its expected short-term, medium-term, and long-term impact on the plant and its ability to manufacture semiconductors.
- The country origin of the cyber incident. Nope
- What kinds of sensitive personal information and/or business information were compromised in the cyber incident.

The CSIRT-CR is also raising the cybersecurity alert level for the Costa Rican manufacturing sector. Internal information at CSIRT-CR indicates that multiple other plants in Costa Rica and surrounding countries use the same Industrial Control System (ICS) cooling software from Cool in the Summer Software (ColdManage v. 2.6).

CSIRT-CR needs to assess the scope of this incident and the responsible parties so it can evaluate cyber risks to other critical manufacturing and infrastructure facilities. Questions include:

- The severity of the vulnerability.
- The exact time Cool in the Summer Software learned of the vulnerability and the exact time the vendor alerted its customers about the vulnerability and the need to patch their systems.
- How many organizations and individuals know about the vulnerability; is it public?

CSIRT-CR has also been alerted to an uptick in malicious cyber activity from China, Russia, and Iran — as well as European cybercriminal organizations — targeting Costa Rican and Latin American semiconductor firms and critical manufacturing facilities. The recipients are encouraged to provide CSIRT-CR with any available information about the possible organizations or individuals behind the ongoing cyber incident at Grupo Rojas Semiconductor Plant.

NEWS BULLETIN

Newspaper: Technology News Now
Headline: Latin America's Growing Role in Semiconductor Manufacturing Highlights Importance of Diversified Supply Chains
Author: María Soto
Date: April 25, 2025

Latin America is emerging as a pivotal player in semiconductor manufacturing. The region's strategic investments and initiatives are reshaping the landscape, emphasizing the need for a diversified supply chain beyond the traditional dominance of Asian manufacturing.

In recent years, Latin American countries have strategically positioned themselves to become key players in the semiconductor industry, aiming to reduce dependence on a single region for critical components and technology. These countries are achieving this through active investing in infrastructure and technology to bolster their capabilities. Brazil, Costa Rica, and Argentina, among others, have implemented policies to attract foreign investment and promote local semiconductor production. These initiatives include tax incentives, research and development grants, and collaboration with international semiconductor companies.

Additional factors to consider include the proximity of some of these Latin American countries to key markets and the increased workforce available. Latin America's geographical proximity to North and South American markets provides a strategic advantage in reducing transportation costs and mitigating logistical challenges associated with long-distance supply chains. Furthermore, these countries have been investing in education and training programs to develop a highly skilled workforce in semiconductor manufacturing.

We will see if these countries are able to keep up with the ever-growing demand of large nations such as the United States. However, it seems as if these nations are taking every step possible to become leaders in the semiconductor industry.

For inquiries, please contact María Soto at msoto@technonews.com or visit technologynow.com for the latest news in technology.

Subject: Disruption to plant cooling operations and manufacturing [URGENT]
To: "Company Leadership" — Grupo Rojas; "Threat Response" — Cirrus Cloud
From: Semiconductor Plant of Grupo Rojas
Date: May 21, 2025, 06:39 AM

Dear Grupo Rojas team, as well as our vendor Cirrus Cloud Solutions,

I am writing to bring to your immediate attention a critical situation that has arisen in our semiconductor manufacturing facility. Our plant is currently facing significant disruption due to problems with the software that we use for managing the cooling systems. Below are the urgent risks we are facing.

Risks:

1. Cooling System Malfunction: The problem has compromised the functionality of our cooling systems, leading to erratic and uncontrolled temperature fluctuations within the manufacturing facility. This poses an imminent threat to the integrity of our semiconductor production processes.
2. Production Downtime: The instability in the cooling systems has forced us to initiate an emergency shutdown of certain manufacturing processes to prevent any potential damage to the equipment. This downtime is resulting in a direct loss of productivity and may impact our ability to meet production deadlines.
3. Equipment Damage: The unregulated temperature variations could potentially cause damage to sensitive manufacturing equipment and tools.

Please be advised that this situation requires urgent attention and a coordinated response from all relevant departments. I will provide regular updates as we work to contain and mitigate the impact of this problem.

We have also requested a threat report from Cirrus Cloud Solutions (copied).

If you have any questions or require additional information, please contact me.

Sincerely,

Jane Smith
General Manager of Semiconductor Plant
Grupo Rojas

Semiconductor Manufacturing Ramp-Up Strategy for Medical Devices and AI in Latin America

January 2025

[CONFIDENTIAL]

Introduction

This document outlines Grupo Rojas' strategic plan to significantly increase our semiconductor manufacturing capacity in the coming months. This expansion is designed to address the growing demand for these critical components in Costa Rica and across Latin America, particularly within the medical device and Artificial Intelligence (AI) sectors.

Current Landscape

The demand for semiconductors in Latin America is experiencing a period of exceptional growth. This surge is primarily driven by:

- The expanding healthcare sector, particularly the increasing use of advanced medical devices that rely on sophisticated semiconductors for functionality.
- The rapid adoption of AI technologies across various industries, all requiring significant processing power facilitated by semiconductors.

Our Commitment

Grupo Rojas recognizes the crucial role semiconductors play in driving innovation and progress in the medical device and AI fields. We are committed to supporting the technological advancements happening in Costa Rica and Latin America by:

- **Scaling Up Production:** We will be implementing a multi-pronged approach to significantly ramp up our semiconductor manufacturing capacity. This may include investments in new equipment, optimizing existing production lines, and potentially establishing new facilities in the region.
- **Collaboration:** We are actively seeking to partner with key stakeholders in Costa Rica and Latin America, including medical device manufacturers, AI developers, and research institutions. This collaboration will ensure that our production capabilities align with the specific needs of the region.
- **Focus on Innovation:** We are dedicated to continuous research and development to ensure our manufactured semiconductors are at the forefront of technological advancements. This will allow us to support the development of next-generation medical devices and AI applications in Latin America.

Initial 2025 investment phase: The company is putting another ₡2,000 billion into the plant and its technology. It is critical this plan moves forward without delay.

Benefits

By significantly increasing our semiconductor manufacturing capacity, we aim to achieve the following benefits:

- **Enhanced Medical Care:** A steady supply of high-quality semiconductors will enable the production of advanced medical devices in Costa Rica and Latin America. This will lead to improved access to life-saving technologies for patients across the region.
- **AI Growth:** Our increased production capabilities will empower the development and deployment of AI solutions in various sectors within Latin America. This will contribute to economic growth and improved efficiency in numerous industries.
- **Job Creation:** The expansion of our semiconductor manufacturing operations will create new job opportunities in Costa Rica and Latin America. This will contribute to the overall economic development of the region.

Conclusion

Grupo Rojas' strategic plan to ramp up semiconductor manufacturing represents a significant commitment to supporting the technological progress of Costa Rica and Latin America. By expanding our production capacity and fostering collaboration, we aim to empower the development of life-saving medical devices and accelerate the adoption of transformative AI solutions across the region. We are confident that this initiative will have a lasting positive impact on healthcare, economic growth, and job creation in Latin America.

MEMO: Latin American Targeting By APT Groups
FOR: Organismo de Investigación Judicial; CSIRT-CR
FROM: United States State Department;
United States Cybersecurity and Infrastructure Agency
DATE: May 22, 2025 Too little too late but help
—

The United States State Department and the United States Cybersecurity and Infrastructure Agency write to nations in Latin America to warn about a recent uptick in activity that suggests an impending attack on Latin America by hostile APT groups. We have detected activity from several APT groups and have conducted a cybersecurity landscape analysis that implies a potential attack on critical infrastructure in Latin America. Several actors involved in the operating of industrial and electrical infrastructure in Latin America may be vulnerable to such an attack.

Potential attacks include (note attacks may be combined):

- Ransomware attack: the encryption of files that render a system inoperable until a ransom is paid.
- Privilege escalation attack: utilizing a vulnerability in software to gain administrative access to other parts of a system.
- Unauthorized access attack: the hidden accessing and copying of files, potentially for a prolonged period.

Likely responsible APT groups include:

- APT-29: an Iranian-backed group that specializes in ransomware attacks.
- APT-16: a group spread throughout Eastern Europe that has frequently targeted small private businesses in Latin America for a variety of attacks. The group is potentially backed by Russia, though this is unconfirmed.
- APT-42: a Chinese group that uses vulnerabilities in industrial control software for privilege escalation attacks.

Help

The US State Department and US DHS CISA are willing and able to help in the case of a cyber incident. We recommend warning actors involved in industrial and electrical activities to ensure their software is patched and that their systems are properly siloed.

From: "Patch Alert" — Cool in the Summer Software Ltd.
To: "Security Updates" — Grupo Rojas Semiconductor Plant
Subject: Vulnerability alert – URGENT
Sent: May 21, 2025, 03:04 AM

Automated patch alert — Priority: HIGH:

We are writing to alert you to a critical vulnerability identified in Cool in the Summer Software's Industrial Control System (ICS) cooling system software provided by our company, which our systems indicate is currently used in your facility.

Vulnerability Details:

- Affected Software: ColdManage (version 2.6)
- Vulnerability Type: Access to administrator permissions underpinning ColdManage software. Risk of attackers deactivating or disrupting ColdManage and the related ICS equipment, modifying settings, or locking out human operators. Risk of attackers then jumping into other parts of the network running ColdManage.

The identified vulnerability allows unauthorized access to the cooling system software, enabling external actors to compromise the integrity of the cooling systems. This unauthorized access may result in uncontrolled temperature fluctuations, leading to potential disruptions in manufacturing operations, or outright disruptions or deactivations of the software.

Attackers could then exploit the access to administrative permissions to jump to other parts of the network running the ColdManage software and the related ICS cooling equipment. Information about the vulnerability has appeared on the dark web, and customers should assume that malicious organizations may have accessed information about the vulnerability.

Patch priority: **HIGH.**

For additional questions and concerns about the patch, please contact:

Jeremy Jones
Lead Software Engineer

Organismo de Investigación Judicial

NOTICE: COLLABORATIVE INVESTIGATION INTO CYBERSECURITY BREACH IMPACTING SEMICONDUCTOR MANUFACTURING FACILITY IN COSTA RICA

May 22, 2025

To the General Public,

We bring to your attention a critical cybersecurity incident that has transpired at a semiconductor manufacturing facility by Grupo Rojas based in Costa Rica.

Incident Overview:

On May 21, 2025, the Grupo Rojas Plant of semiconductor manufacturing fell victim to a targeted cyber-attack, exploiting a vulnerability in its cooling software. This breach has resulted in immediate disruptions to plant operations and has sparked concerns about potential long-term consequences on the semiconductor supply chain, impacting essential industries such as automotive and healthcare.

Collaborative Investigation:

In response to this alarming incident, law enforcement agencies across Latin America are joining forces to collaboratively investigate the source of this cyber-attack. The primary objective is to identify the foreign actors responsible for this breach and take appropriate legal actions against those involved.

Public Cooperation:

We seek the active cooperation and support of the public in providing any information or assistance related to this investigation. If you have observed any suspicious activities or possess relevant information, please contact your local law enforcement offices (please contact the OIJ if you are located in Costa Rica).

Transparency and Updates:

To maintain transparency, regular updates on the investigation progress will be shared with the public. We appreciate your understanding and patience as we work diligently to address this cybersecurity threat.

Thank you for your attention and cooperation.

Sincerely,

Organismo de Investigación Judicial

Technical Report: Cybersecurity Incident Impacting Cooling System Equipment

Grupo Rojas
May 22, 2025

Overview: This report outlines the technical details and consequences of a recent cybersecurity incident that has affected the cooling system equipment at our semiconductor manufacturing facility in Costa Rica. The incident occurred on May 21, 2025 and has resulted in both operational disruptions and physical damage to critical cooling components.

Incident Description: The cyber-attack exploited a vulnerability in the external cooling software, supplied by Cool in the Summer Software Ltd., used to regulate and monitor our plant's cooling systems. As a consequence, the compromise of the software not only disrupted normal operations but also caused physical damage to certain cooling equipment. The nature of the damage extends beyond the software layer, impacting the hardware components responsible for maintaining optimal operating temperatures within the facility.

Physical Damage Assessment:

1. **Chilled Water Pumps:** The attack caused an overload on the chilled water pumps, resulting in mechanical failures. Preliminary assessments indicate that some pumps have sustained damage beyond repair, requiring replacement.
2. **Heat Exchangers:** The compromise of the cooling software led to erratic temperature control, causing stress on heat exchangers. Visual inspections reveal signs of overheating and potential structural damage that may compromise their efficiency and overall functionality.
3. **Cooling Towers:** The cyber-attack disrupted the normal functioning of the cooling towers, leading to fluctuations in water circulation. Initial inspections suggest wear and tear on key components, affecting their ability to dissipate heat efficiently.
4. **Control Systems:** The compromised software not only disrupted the operational parameters but also interfered with the control systems governing the entire cooling infrastructure. Some control modules have suffered irreversible damage, requiring replacement and reprogramming.

Potential Financial Impact: Assessments are still in progress, but the initial numbers suggest it could cost tens of millions of colóns, at least, to replace the equipment. The plant previously announced its intention to invest another ₡2,000 billion in January of 2025 in the plant (see: Semiconductor Manufacturing Ramp-Up Strategy for Medical Devices and AI in Latin America, January 2025).

Impact on Operations: The physical damage to the cooling system equipment poses a significant challenge to the prompt restoration of normal operations. Due to the specialized nature of the cooling components and their critical role in semiconductor manufacturing, sourcing, and replacing the damaged equipment will not be a quick and straightforward process. We may need to import many replacement components from abroad, which will add to remediation costs.

Challenges and Mitigation Efforts:

1. **Equipment Procurement:** Given the specialized nature of semiconductor cooling equipment, sourcing compatible replacements may involve lead times that could extend the downtime.
2. **Technical Expertise:** Repairing or replacing damaged components will require specialized technical expertise. Collaborating with the original equipment manufacturer (OEM) or certified service providers will be essential to ensure proper installation and configuration.
3. **System Calibration:** Following equipment replacement, a thorough calibration process will be necessary to ensure the restored cooling system operates within specified parameters, maintaining the integrity of semiconductor production processes.

Recommendations:

1. Engage with OEMs and certified service providers for expedited procurement and installation of replacement equipment.
2. Collaborate with cybersecurity experts to reinforce the resilience of our cooling system against future cyber threats.
3. Communicate transparently with relevant stakeholders, including production teams and management, about the expected downtime and recovery plan.
4. Prioritize the implementation of additional cybersecurity measures to prevent similar incidents in the future.

This report aims to provide a comprehensive understanding of the technical aspects of the cybersecurity incident and its impact on the cooling system equipment. The collaboration of all relevant teams and stakeholders is crucial to ensure a swift and effective recovery process.

Please do not hesitate to contact me to further discuss our findings and next steps.

Sincerely,

Jane Smith
General Manager of Semiconductor Plant
Grupo Rojas

From: Loretta Cline— CSIRT-CR
To: Paolo Gonza — OIJ
Subject: Fwd: Cool in the Summer Global Software
Sent: May 20, 2025, 03:23 PM

Paolo,

Just thought you should see this…any thoughts?

~ Loretta

Begin forwarded message:

From: Subject: Sent: Hans Rosling — Cool in the Summer Software
To: Loretta Cline — CSIRT-CR
Subject: Cool in the Summer Global Software
Sent: May 20, 2025, 11:59 AM

Dear Loretta,

Thank you for your email concerning other users of our Cool in the Summer ICS software. Unfortunately, we are only able to provide a partial list of the end users of our software. We sell our software to several ICS manufacturers for them to integrate it into their hardware. We supply security patches to those hardware manufacturers and they then manage the updates to their customers. We are currently reaching out to our customers to determine the identities of the end user companies. As of now, we know that the following plants currently use the vulnerable version of the software:

Perfect Semi, Inc	United States
Binary Chips	Vietnam
Ohm's Wafers	Taiwan

The following plants might use the software (we no longer list them as an active customer, but it is possible that they still use the hardware that our software is preloaded on.

Costa Rican Conductors	Costa Rica
Arizona Silicon Suppliers	United States
Chip Testing, Inc.	Mexico

We're still tracking down how the vulnerability got into our system, but it's possible it derives from the open-source software that we utilize Tafron5, as is commonplace in the industry. Also, we believe several ICS companies integrate this software into ICS

products sold to power plants even though we have told them that is not an intended use. We are trying to determine where the software may be being used in power plants.

Please let us know how we can be of further assistance to CSIRT-CR.

- Hans

From: Sommer Citruh — Grupo Rojas
To: Jeff Sullivan— Grupo Rojas
Subject: Re: IT Review
Sent: May 5, 2025, 04:11 PM

Jeff,

I spent the past day checking log files, and I'm not sure how we got so far behind. Some of the firmware running our industrial hardware is several months out of date—specifically the ones that come pre-installed with the software rather than the software we install and manage ourselves. There's one piece of software from Cool in the Summer that hasn't had a routine patch in almost a year, and Cool in the Summer's software is present in nearly all of our industrial control systems (and I assume other firms). Not sure how much we can trust their code…

Since we don't have logical control over a lot of these machines, we would have to go through the hardware vendor, I assume. I'm also noticing a lot of old users with administrative access who are still using the default password. !!!

I strongly recommend we shut down our network for a day or two while we get this resolved., even if plant operation is stalled. Have you escalated this to leadership? Help from Cirrus would be ideal.

~ Sommer Citruh
—
Sommer Citruh
Senior IT Officer
Grupo Rojas

Begin forwarded message:

From: Jeff Sullivan — Grupo Rojas
Copied: Paul Gold, Business Strategy — Grupo Rojas
To: Sommer Citruh — Grupo Rojas
Subject: IT Review
Sent: April 26, 2025, 07:39 AM

Sommer,

I've heard rumblings on cybersecurity listservs about a potential infrastructure-based attack on Latin American countries. The business strategy team is a little concerned given our impending investment plans, do you think it would be worth moving up our annual cybersecurity review? Could you do a quick landscape analysis today and give your thoughts?

- Jeff