RMI Insight

PROFESSIONAL SECURITY SERVICES

FALL 2024 / RMI INTERNATIONAL INC.

Happy Holidays from RMI

Dear Team,

As the holiday season arrives, I want to extend my sincerest gratitude for your incredible contributions throughout the year. Your hard work, creativity, and commitment have been the backbone of our success, and I am truly thankful for each one of you. This year has brought its own set of challenges and achievements, and together, we've navigated them with resilience and teamwork. It's your dedication that makes our company a great place to work, and I am proud to be part of such a remarkable team.

As we celebrate the holiday season, I pray that you find time to relax, recharge, and enjoy your time with your family and friends. May this season bring you joy, peace, and a sense of fulfillment. Let's cherish the moments of happiness and reflect on our accomplishments. As we look forward to the new year, I am excited about the opportunities that lie ahead and confident that, together, we will continue to achieve great things.

Wishing you all a Merry Christmas and a prosperous New Year filled with health, happiness, and success. All the best and God Bless.

Rick Rodriguez, Sr. PPS
CEO/ Founder
RMI International Inc.

Spreading the Cheer at Hillsdale's Shopping Center

On Friday, November 15th, Hillsdale Shopping Center in San Mateo, California held their annual Christmas Tree Lighting Ceremony.

The event was estimated to have hosted thousands of shoppers who enjoyed the kickoff of the 2024 holiday season.

The RMI team did a great job assisting with the event logistics and working alongside San Mateo Police Department to ensure the event remained safe.

Left-Right: Michael Costa (RMI account Manager), Peter Lee (Security Director, Hillsdale Shopping Center / Northwoods Retail), Lt. Anthony Riccardi (San Mateo Police Department), Serah Larison (RMI President), Rachael Paniagua (RMI Business Development), Sgt. Lupe Mejia (San Mateo Police Department).

Left-Right: Norma Moran (RMI Customer Service Representative) and Rachael Paniagua (RMI Business Development).

RMI Customer service representative, Norma Moran, participated in the Tree lighting event as Ms. Klaus and handed out free 3D glasses to children to enhance the tree lighting experience. Great work RMI team!

Safety Corner

Fall and Winter Safety Concerns

The elements, the reduction of natural light and other seasonal concerns can make this time of year particularly hazardous regarding slips, trips and falls.

Therefore, it is important to keep the following in mind:

- Watch your step. Rain, snow, ice, and other conditions can make walkways, parking lots, and other foot traffic areas slippery.
- Stay alert for others who may be distracted and/or having difficulty seeing you while driving and take precautions as necessary.
- Monitor for lighting problems and have a back-up source of light, such as a flashlight, available as required.

If a hazardous situation is discovered, note it, report it, and help guard against a mishap, as best as possible, until the problem is corrected.

Sincerely,

Richard Aparicio
RMI Senior HR Manager

RMI INTERNATIONAL

8125 SOMERSET BLVD.
PARAMOUNT, CA 90723

TEL (562) 806 - 9098
FAX (562) 806 - 7017

WWW.RMIINTL.COM

In Recognition Of

On behalf of the entire RMI and Honda Corporate Security team, we want to express our deep admiration and thanks for Francesca Fermano's remarkable contributions to the workplace. She consistently goes the extra mile to support her colleagues and vendors, and we are grateful for everything she has achieved over the past year.

Her countless hours of dedication and unwavering professionalism have inspired and motivated
the entire RMI and Honda team.

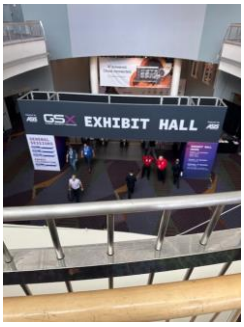
As the ComSec Supervisor, I wholeheartedly appreciate her hard work and commitment to making every critical project a resounding success. Francesca's uplifting spirit lights up the office, and her positive attitude continuously inspires her team. We are truly fortunate to have her with us!

As always, we look forward to Francesca's continued excellence. Her radiant personality makes each day at work a pleasure! Continue your excellent work!

Greg Soles
RMI-Honda COMSEC Supervisor

ASIS – GSX Conference, Orlando FL

RMI Senior Manager, Kimberly Kirk, was invited to attend the GSX Conference in Orlando, FL, hosted by ASIS International with Honda executives from Monday, 9/23/24 to Wednesday, 9/25/24.



GSX Exhibit Entrance

The Global Security Exchange (GSX) Security Conference is held every year and brings security professionals together from around the world to grow in the ever-changing security industry. GSX provided training sessions on the latest security trends and evolving security technology available today.

The training sessions covered areas in security service-related topics such as behavior threat detection, organizational risk analysis, active shooter response, and enterprise security risk management (ESRM).

Vendors Showcasing Area

Training also delved into employee-based areas such as today's workforce and the best practices for managing security officers with new technology.

Additionally, an exhibit hall was set up for all vendors to showcase their security business or product for all attendees to network for future business. Vendors presented their products such as access control systems, personnel safety, cyber security, physical security, and advanced AI technology.

All attendees could network with security professionals from different companies and sectors in security from all over the world. The conference was a great opportunity for RMI and Kimberly was excited to learn from the experience.

Threat Detection Training

Kimberly attended training sessions each day and visited many vendors to bring back the knowledge she gained from the GSX conference.

"When you lose sight of the customer, you've lost your vision for the future." – Rick Rodriguez

"Success can only be achieved by working towards a common goal." – Serah Larison.

AI Powered Scams & Fraud (LMG Security Webinar 10/16/24)

Hackers are becoming more creative, crafty, bolder, and successful with each passing day in finding ways to access the personal data of businesses and others for purposes of fraud and to cause other harm. Therefore, it is important for all to be ever-vigilant to not become a victim and to help not put others (friends, coworkers, company, etc.) at risk.

Methods of Attacks:

- AI Generated Videos and Audio: These are created through programs like HeyGen, etc., impersonating someone you trust – CEO, HR, Payroll, your Bank Rep, etc. – to get you to join a Teams meeting to divulge sensitive information, or to release personal financial information, etc.

- AI Generated Fake Emails, Texts, and Websites: These are created to get you to click on a link or to get you to visit a website they have created that mimics the real thing in order for them to place cookies on your computer granting them access to your email, company files/information, passwords, etc.

Once they have gained access, they can analyze the data to set up fraudulent vendors in place of your real ones, while limiting the real vendor's access to you, in order for you to unknowingly pay the hacker instead.

- Voice and Mobile Device Attacks: Hackers using AI software can clone your voice by recording your personal voice mail answering message, recording any audio messages you post online, or by listening to your conversations. It doesn't take much for their AI programs to assess your voice patterns, speech, etc., for creating fake messages purportedly from you and sent to scam your trusted contacts.

  For instance, hackers have been using scams by pretending to be a trusted contact sending a voice message that sounds like a trusted source to get a person's colleagues or friends or other personal associates to take advantage of *this great business opportunity*, or that *great deal* (gift cards, etc.) or to breach their victim's personal security (*This is bank X. We detected unusual activity in your account. Please follow this link to verify your identity. https://xxy.com*) by having the victim access the fake link or visit a fake website and following their prompts.

- Generated Fake QR Codes: Fake QR code use is on the rise. One example is where hackers affixed fake QR codes to parking meters for "easy payment". However, these had nothing to do with paying your parking fees and everything to do with them accessing your credit cards or other payment source.

  If you were not paying attention, you may have become taken advantage of twice – paying for something you thought you were purchasing and receiving a ticket for not paying for your parking. Fake QR Codes are also being used on some gas pumps.

How to Protect Yourself and Your Organization:

- If you are not expecting it, (invoice or other odd request even if from a "trusted source"), it might not be legitimate. As necessary, reach out first via a trusted means of communication for confirmation before accessing, complying, etc.

- If it looks fishy, it may be phishy. Check the email contact identity (looks like trusted source but email name is off by one letter or number, etc.), website address (site name looks the same but off slightly), log-in page set-up looks different than what you usually log into, etc. If it looks different than what you are used to, reach out first via trusted means for confirmation before accessing.

- If you have not seen the QR code before and/or have not safely used it, then pay the old trusted way and/or reach out to a trusted source to verify first.

- Consider using multi-factor authentication where offered/available for extra protection – through your I.T. Department, bank, etc.

- If your Spidey Senses are tingling, listen to them – *this video looks like my boss and almost sounds like my boss, but something is off. I think I will call him/her first before I do what they are asking*.

- Advise new personnel of who to trust and how to recognize who is not part of the organization.

  Note: RMI will never require staff to send personal information via email or web link.

If you become aware of someone gaining access to your personal or company business data without authorization, via your cell phone, tablet, computer or other means, then it is important for you to take measures as soon as possible to help reduce the negative impact, to yourself or others, by reaching out to the respective institution or your company supervisor and IT for assistance.