RMI Insight

PROFESSIONAL SECURITY SERVICES

FALL 2025 / RMI INTERNATIONAL INC.

Warm Holiday Wishes from RMI!

Dear RMI,

Team, as we approach the holiday season, I want to take a moment to express my heartfelt gratitude for your hard work and dedication throughout the year. It is due to your efforts that RMI has been successful. I have recently enjoyed traveling to visit some of our work locations and recall with fond memories the days I wore a security uniform.

I plan to continue my site visits in 2026 and look forward to seeing more of you.

My wife Lupe and I hope that you have a holiday season full of love and special moments with family and friends. We wish you a Merry Christmas and Happy New Year!

Always forward,

Rick Rodriguez
RMI CEO & Founder

A Job Well Done!

On October 15th, RMI recognized the following ComSec staff for their professionalism and teamwork displayed when managing two emergency incidents on October 8th, 2025.

Irene Pech quickly informed the client of the situation and followed instructions precisely on the follow-up actions.

Irene's clear communication helped ensure a smooth and coordinated response.

Francesca Fermano displayed excellent leadership and awareness in the control room.

Francesca had all the information ready, addressed every question and concern with confidence, and set the tone for how these situations should be managed.

This is the type of teamwork and readiness that keeps our clients safe. Well done team!

From Left to Right: Francesca Fermano (ComSec Assistant Supervisor), Rick Rodriguez (RMI CEO), Irene Pech (ComSec Operator), Kim Kirk (RMI Sr. Account Manager).

Safety Corner

Housekeeping

RMI wishes to remind all personnel to maintain their posts in a neat and orderly manner for their safety and the safety of others who may visit their post.

Important things to remember are:

- Ensure that cupboard doors, desk and file cabinet drawers, etc., are closed when not in use to help prevent someone from bumping into them and injuring themselves.
- Ensure fire extinguishers, if posted, are not obstructed and are visible in case they are needed.
- Ensure exits remain accessible in case of emergency.
- Ensure trash does not build up and overflow the receptacle.

If you encounter a housekeeping problem you are unable to easily and safely correct yourself, then you will need to report the problem to your supervisor as soon as possible, document the issue, and follow-up until it has been corrected as needed.

Sincerely,

Richard Aparicio
RMI HR Director

RMI INTERNATIONAL

8125 SOMERSET BLVD.
PARAMOUNT, CA 90723

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

WWW.RMIINTL.COM

All is Merry & Bright at the Hillsdale Shopping Center

On Friday, November 21st, RMI President, Serah Larison, had the pleasure of joining the RMI and Hillsdale team to celebrate the start of the holiday season with the Hillsdale Shopping Center's Santa's Christmas Tree Lighting.

This year the theme was "The Nutcracker." Guests were entertained by the San Francisco Youth Ballet who performed highlights from The Nutcracker Ballet. RMI's team did an amazing job assisting with all the logistics of the event, most importantly keeping Santa safe.

Great job team and Happy Holidays!

Serah Larison (RMI President) and Peter Lee (Hillsdale Security Director)

Have you seen RMI's CEO?

This fall, RMI's CEO, Rick Rodriguez, went on a tour of RMI service locations. During his site visits, Rick had the pleasure of meeting with both RMI employees and clients. Where will Rick visit next? See you in 2026!

Rick with Calvary Chapel Downey Officer, Luis Perez

Rick with Honda Irving Security Supervisor, Terrion Cameron, and Officer, Aidan Luna

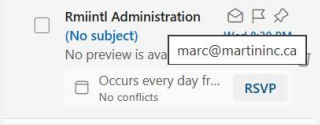
Rick and Torrance Security Officer, Mervin Smith

Rick and Honda Corporate Security Manager, Rob Bibart

Cyber Threats – Protecting Yourself & Others

Cyber threats are becoming increasingly sophisticated, and they are on the rise, resulting in harm to the wary as well as the unsuspecting. Hackers employ their tactics for various reasons such as to harm one's reputation, scam others out of money, etc.

It's not just businesses that are their targets. Anyone with a computer, tablet, or smartphone can become their victim, so it is important to be aware of their schemes and work to guard against them.



Phishing email sent to RMI EEs on 11/12/25.

See Cyber Threats, continued on p3.

Continued from p2.

Cyber Threats

I. Cyber Threats

- Impersonations: The ability of scammers to impersonate another using apps like HeyGen, etc., has improved significantly and they are continuously working to remove the bugs out of their schemes. All they need is a few images of you and/or a short sample of your voice from an online post, voice mail, recording of a call they make to you, etc., to impersonate you.

They do this for various reasons, such as:

  - To create a video or video call pretending to be a CEO who is making a plea to company personnel for them to visit a fabricated "charitable website", and donate money for some "worthy cause".
  - To call you pretending to be a loved one or friend in "dire straits" who needs money as soon as possible to get them out of a "bad situation" (travel nightmare, bail, etc.).
  - To call you pretending to be a trusted other such as your company payroll rep, banker, realtor, etc., to trick you into providing personal, sensitive information to stop some sort of imminent harm from occurring to you or to help you in some time-sensitive, beneficial way.

- Phishing: Hackers can use malicious AI programs like Worm GPT to create a phishing email in seconds. They can also create fake websites to mimic legitimate ones very quickly.

  They then send you their phishing emails, texts, and chats to access your system, after you've accidentally clicked on a malicious link, enabling them to locate financial transactions and other sensitive/personal data in your system, to redirect your funds, personal, or business info, etc., to them.

  For instance, AI can quickly sort through and assess message content, grab attachments such as invoices, etc., to determine the from/to who and why, to then create a fictitious correspondence redirecting you to pay them instead of the proper recipient by pretending to be your trusted contact who says something like, "A billing error has been made, please direct your payment to this account….". They can also offer you a fake number or other contact method for reaching out to them.

II. Protecting Yourself & Others

- Video Impersonations: If you receive a video call claiming to be from someone you know or someone in your business world asking you to do something for them, look for clues that this might not be legit such as quirks about their face and body movements that don't match up to how they normally are. Ask them to stand up and move about in real time to see if it is the real person.

- Voice Impersonations: If you receive a call from someone who is claiming to be a person you know asking you for something, listen to their voice and how they speak to see if this does not represent who they are. Ask them a question that only the real person would be able to answer and recontact them, if possible, at a trusted number to verify them and their request before acting.

RMI INTERNATIONAL

8125 SOMERSET BLVD.
PARAMOUNT, CA 90723

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

WWW.RMIINTL.COM

- Phishing: Never click on a link or provide sensitive personal or business information if you cannot first confirm/verify the source and reason as legitimate.

  If you are unsure, contact the party via a safe/legit means (known contact number, secure website, etc.)

  Remember, if it looks fishy, it may be phishy.

III. Reporting Incidents

- Reporting Malicious Activity: If you have been scammed, or even if you believe you have been scammed in one manner or another, it is important to report this to the proper authority as soon as possible.

  If it is work-related, report the details to your supervisor immediately for them to run it up the chain (management, IT, etc.) as soon as possible and document it.

  If you believe you have been scammed personally, you are encouraged to also report this to the appropriate party/institution (bank, governing authority, family/friend also affected, etc.).

(Info from LMG Security Webinar 10/30/25)