Some boating regions of the country are experiencing a spike in thefts of marine equipment ranging from electronics, outboard engines and lower units to entire vessels. While some boaters are calling for manufacturers to install GPS trackers and security codes in electronics, these actions may have negative consequences.

Disappearing

Marine electronics industry seeks solutions to MFD thefts

For boat owners the pit in their stomach will be just as deep and dark as the jagged hole left in the helm, after some creep ripped the MFD out of it. A mix of rage and despair follows any criminal violation of personal property. But boats are particularly vulnerable, and theft from boats can be particularly hurtful. It's also becoming so commonplace in some areas that boaters are crying out for help from the community at large—and from electronics manufacturers.

The theft of electronics from boats has been a problem for as long as electronics have existed, but there seems to have been a spike in recent years. Not only are more and more boats being raided while they sit at the dock, thieves have even taken to cutting holes into the walls of buildings to steal electronics en masse from distributors.

BY

Statistics should reflect this recent surge of criminal activity, but unfortunately there are no statistics. While the theft of boats is tracked, there's no national database of thefts from boats. And according to BoatUS Special Investigations Unit (SIU) Director Rich Carroll, the vast majority of stolen electronics are related to boat theft in general simply because electronics are attached to a boat that gets stolen. After a boat is taken, it's rare to recover it with the electronics intact. Most of the stolen electronics appear to be MFDs—multi-function displays, although no onboard electronics are immune.

While Carroll says they haven't seen a drastic increase in incidents of pure electronics theft, at certain times in certain places it may seem like that's happening because there are pockets of intensified activity. These spikes of thefts in specific locations tend to be clustered where the most boats are found.

"The bad guys go where the opportunity is," Carroll says. "That may make it appear like electronics theft is rampant in specific states, but when you consider the volume of boats in any particular state, the problems are actually fairly consistent across the board."

Electronics theft has become so prevalent in some areas, however, that victims have taken to social media in an attempt to help each other combat it. *Facebook* has become the main platform, and now has groups like "Stolen Boats and Motors in Florida," and "Bahamas Boat Theft and Security Information." Mem-

bers post pictures of stolen boats, electronics, and outboards—lower unit theft remains a similar criminal niche market—and share them as much as possible in the hopes of recovering goods or finding potential witnesses.

"I applaud the various groups on social media that are both driving attention to the electronics/gear events with discussion on options as well as becoming a resource for active boat theft scenarios," says Brian Kane, Chief Technology Officer for boat security system manufacturer GOST Global.

"Social Media has played a great part in helping to recover stolen boats, identify thieves, and keep a pulse on theft issues. Remember the Lumitech boat from a few years ago?" he asks.

The boat Kane's referring to was Lumitech's demo boat, a triple-engine center console Intrepid, which was stolen just before the IBEX show. The company went to social media, the story went viral, and an estimated quarter-million people became engaged. Within 36 hours a lead developed, and soon thereafter the boat was recovered. Success stories like this are limited. As often as not boats are recovered with all their electronics gone and/or the engines missing.

Talk of the town

Spend some time on these sites, and one thing quickly becomes evident: the public is crying out for electronics manufacturers to help combat this problem. GPS trackers, unlock codes, and other theft deterrents are popular topics of conversation. And the conversation is loud enough that NMEA is hearing it.

"Some of the suggestions may be viable options," says Mark Reedenauer, NMEA President & Executive Director. "NMEA wants to involve all the MFD manufacturers in a discussion, so constructive ideas can be put on the table. While some of these ideas seem viable at the surface, when you start peeling back the onion, extensive costs could be added. So this needs to be carefully examined. The NMEA Installation Standard Committee plans to include additional safeguards to the physical installation of an MFD, such as through-bolting, rear-mounting etc., which can deter theft because of the additional time it takes to remove the equipment."

Reedenauer also says that the issue has two different angles: consumer theft in which the boater suffers the loss, and volume theft, in which the distributor and/or dealer suffers the loss. He says that NMEA plans to address both issues, with member participation via conference calls and in-person meetings. (One call session occurred in early January involving more than a dozen participants. An in-person follow-up meeting is planned for the Miami International Boat Show in mid-February.)

"We would like to approach this as a team," he says. "While NMEA has to first and foremost be very careful not to tell any member company or individual how to run their business, we do hope to address this."

Kane agrees this approach is a good idea, and believes that the more layers to security there are, the better. "If there are security options that MFD manufacturers can look into, that's a welcomed addition," he says. "Security systems are still going to be a first line of defense. We've seen and heard a lot of stories over the years [at GOST]. It's not uncommon for a client to call us the day after a theft attempt on their boat to tell us that the electronics and gear were stolen off a bunch of boats around theirs, before their GOST system scared the dirt bags off the docks. Additionally, cameras with offsite streaming video are a valuable tool to capture events and send motion notifications to clients. However, cameras are not security. We encourage enabling additional security systems on the equipment aboard the boat to defend against theft. And we appreciate boat builders who build security features into their helms, such as installing a clear plexiglass case over the electronics or even a pop-up fiberglass cover. Both of these examples allow GOST to place a covert contact sensor that will fire off an alarm when opened."

Tracking the options

While marine manufacturers seem to have an open mind about how to approach enhancing the security of their MFDs, they do naturally see the issue from a slightly different perspective.

"We're not dancing around this issue or trying to avoid it," says Dave Dunn, Garmin's Director of Sales and Marketing for Marine. "But this isn't so easy to do. A lot of people are demanding trackers, for example. They have trackers in their phones, but they already pay a monthly service fee for those to be activated, and someone has to pay for that type of service. The companies mak-

ing the phones have a very different economy of scale (millions of units, versus tens of thousands) so they pay a lot less for the hardware. And don't forget that iPhones still get stolen, too."

Kane understands the same issues with GPS trackers, but also sees opportunity. Thieves find weaknesses quickly and counter-measures may be relatively easy. "If MFD manufacturers are putting in the communication equipment, how long before the bad guys figure out where the necessary battery backup or SIM card is located? How long before they figure out how to remove it while the unit's powered down?" he asks.

"As cellular becomes cheaper and faster there is potential value for manufacturers to embed this technology in future product road maps recognizing the benefits of telematics, remote updates and overall user experience improvements. It will come at additional hardware/airtime costs and the consumer has to understand that nothing is foolproof."

Then there's the question of what would happen once a unit is stolen. Who's in charge of monitoring for stolen MFDs, the manufacturer or the end user? Part of the issue is that some level of responsibility lays with the consumer, at least as much as it does with the manufacturer. And consumers can at times be surprisingly lackadaisical until theft affects them personally.

"All of our major products have individual serial numbers on them," points out Jim McGowan, Raymarine's Marketing Manager. "In theory if someone registers their warranty with us, we can link a product to an owner by that number. Unfortunately, though, not many people take the time to register. We also have product shipment history linked by serial number. That tells us what dealer or distributor originally took delivery of that item from Raymarine, which could possibly help to narrow down the owner of an item if it was recovered by law enforcement. But the effectiveness of the shipment history varies widely depending on whether the item was shipped to a mom-and-pop-type marine electronics dealership, versus a wholesale distributor or big-box marine retailer."

As it turns out, this rather old tech form of tracking units is also among the top practices encouraged by law enforcement, though with a new techy twist. "Overall percentages of recoveries are extremely low, however, victims may be able to improve this by helping us identify their items," says General Investigations Unit Commander Katherine Baker of the Miami Police Department. "Often items are pawned or sold to second-hand shops. Without serial numbers or unique identifying features, there's no way to verify ownership during inspections.

One way of doing so is by keeping detailed records of items and/or utilizing record-keeping applications such as 'ReportIt.' ReportIt is a Citizen Property Inventory System powered by Leadsonline. It provides a secure online record of valuable property accessible from anywhere, and assists law enforcement with the recovery of stolen property. Individuals can upload serial numbers, distinctive markings/pictures, etc., which can be later provided to the authorities during reporting," she says.

The problem with locking codes

On the surface, locking codes seem like another realistic option. But these, too, have a number of pitfalls.

"Locking codes are a viable option," says Dunn. "But we want our users to have a good experience, and making them user-friendly is

Preventing thefts

After a rash of theft incidents occurred along the I-95 corridor in 2017, including thefts targeting electronics as well as outboards and boats in general, BoatUS issued several tips including these:

- Take a look at your storage area. Lighting, motion-operated lighting or audible alarms, difficulty in gaining entry, video surveillance, and signage advising that license plates are being recorded with video surveillance should all be considerations.
- Slow the thieves down by having electronics protected by a locked solid cover, and use tamper-resistant fasteners for mounting.
- Make stealing electronics less appealing by engraving and posting a warning. Create and keep a list of serial numbers, and take pictures of the units.
- Be wary of suspicious questions. In most thefts from dealerships during this spate of incidents, a suspect posed as a boat shopper the day before the theft occurred. Boat owners should remain cautious about questions from strangers wanting to know about access, and get to know their dock neighbors so they can more readily recognize suspicious activity and people who don't belong.
- Consider adding a boat tracking device that will sound an early alarm if something goes amiss.

While a group of industry players and NMEA search for solutions to guarding against electronics thefts, the answer in some, although certainly not all, situations may be to make MFDs easily removable so owners can take them home. Meantime boaters are advised to keep their insurance policies up to date.

not so easy. What happens when someone forgets or loses the code? What if the marina needs to run your boat? The obvious solution to those issues is to have a dealer master or bypass code, but if we did that, the information would probably get out onto the street in five minutes flat. We need to look at this from every possible angle, and come up with creative ways to attack this problem."

Kane also feels locking codes offer some good possibilities, but sees similar issues and also points out that if someone operates the boat without being able to use the electronics and they run aground because of it, a whole new can of worms regarding fault could be opened up. A possible answer may be a minimal functionality screen, while anything beyond that requires a passcode entered at startup. But that still would require a master reset to cover forgotten codes, or new owners. And like Dunn, Kane points out that any secret sequence or code used to reset a unit will eventually be figured out by the bad guys.

Dunn says that Garmin considers this issue a top priority, and they are already testing some possibilities. Another company we spoke with that has already begun moving forward with additional security measures is Furuno.

"Our software engineers are in the process of implementing password locking functions for future software versions," says Jeff Kauzlaric, Furuno's Advertising and Communications Manager. "They will be implemented in new MFD introductions and I believe will be retrofitted to some current MFD software. This will hopefully reduce theft."

Kauzlaric also says, however, that they haven't yet settled the issue of how to reset passwords, especially if there is no internet connection.

No final solution?

Virtually everyone agrees that there will never be a final solution to the theft issue.

"Admittedly this is a sad problem, but it's not going away," says Carroll. "Much of this battle is making your boat less attractive to thieves. Making them go somewhere else. All you can do is try to stay one step ahead."

Interestingly, he also suggests taking an approach opposite to that of many installers: instead of making it more difficult to remove the electronics, make it a whole lot easier so that owners can take them home when leaving the boat. Obviously, this works well for those with binnacle-mounted units, but some sort of quick-release mechanism for flush-mounts could prove an effective way of preventing theft, too. When all is said and done, however, perhaps not too surprisingly, in Carroll's opinion the ultimate backstop is a good insurance policy.

Another potential creative security measure that Kane suggests is utilizing blockchain technology. Blockchain is a shared and constantly updated digital record of transactions, and is best known as the virtual "ledger" used for digital currency including Bitcoin. At the very least, this could create a universal registration system while maintaining confidentiality.

As is often the case with any security matters ranging from boat theft to national defense, all of us are in an arms race with the bad guys. But hopefully, with inter-industry cooperation, support from the consumers, and some creative thinking, it's an arms race that the criminals will lose.

About the author