Cyber Risk Management for Marinas

December 2024
Docks Expo

PRESENTATORS:
Lori Sousa - Sea Land Insurance Corp.
Joe Revier - Slipify

SEA LAND INSURANCE CORP

slipify better marina software

Today’s Presenters

Lori Sousa
President, Sea Land Insurance Group

Lori Sousa, CMIP, is a seasoned insurance expert specializing in risk management for small businesses. As a Certified Marina Insurance Professional, she provides tailored solutions to help marinas address unique and evolving risks, including cyber liability.

Joe Revier
Co-founder & CEO, Slipify

Joe Revier is a tech entrepreneur and former US Marine and cyber security operator. As a co-founder of Slipify, he brings expertise in developing intuitive, cloud-based tools that help marinas streamline operations and navigate modern challenges.

Today’s agenda

What is cyber security?	10 min
How is it relevant to me?	10 min
What can I do about it?	10 min
Ransomware scenario	20 min

What is cyber security?

What comes to
mind when you hear
“cyber security”?

What comes to mind for me?

What comes to mind for me?

What comes to mind for me?

Cozy Bear

- Sophisticated **cyber espionage group linked to Russian** intelligence agencies
- Known for targeting government, military, and corporate entities worldwide, they specialize in stealthy operations, including spear-phishing campaigns and exploiting software vulnerabilities to steal sensitive data

Cyber warfare has been happening for decades

Stuxnet example:

- US-Israeli operation to destroy Iranian nuclear processing capabilities
- Infected industrial control systems that refined nuclear materials
- Overloaded those systems to destroy the materials and the facilities making them

What *else* comes to mind for me?

Cozy Small Business Owner

- Not thinking about cyber security because they aren't a massive company or government
- Worried about a thousand other things but doesn't think twice about using "password123" for their bank login

How is it relevant to me?

Even the smallest businesses have something cyber criminals want.

Money

- Bank Accounts
- Payment processing platforms
- Customer account details
- Your cash

Complex attacks are more common and easier to conduct than ever before.

Today, anyone here can go on the internet or dark-web and buy:

- Compromised credentials
- Programs that automate hacking
- Services that will perform attacks for you
- Existing compromises
- Fake IDs and documents
- Temporary or spoofed email accounts

Modernizing your operations is becoming more necessary, but it comes with new risk exposures.

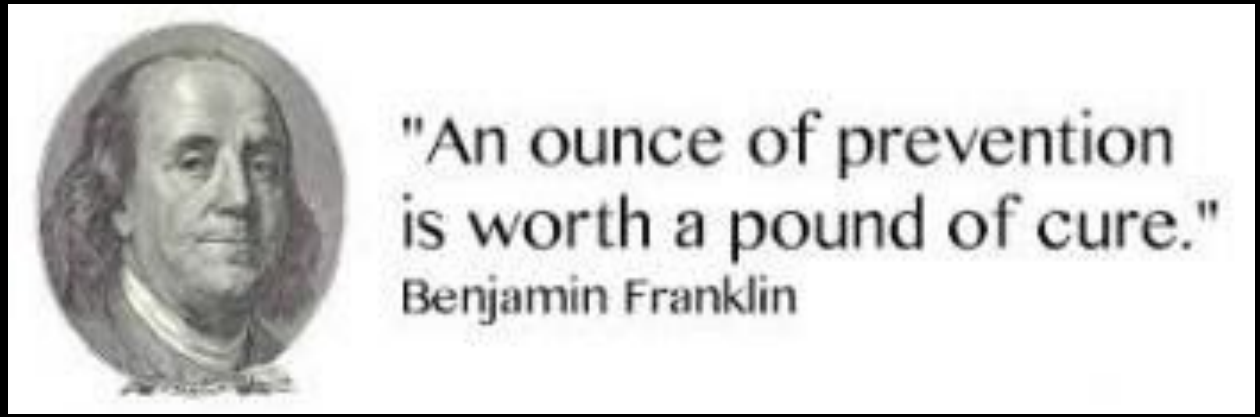
What can I do about it?

Cyber risks are just another risk to be aware of when operating a business.

Inherent Risk	-	**Mitigations**	=	**Accepted Risk**
Risk that is a natural part of your business operations		Actions you take to protect yourself from those risks		The remaining risk that you are okay with to operate

Most businesses are victims of opportunity.

A little bit of effort today can prevent orders of magnitude more effort after an incident.



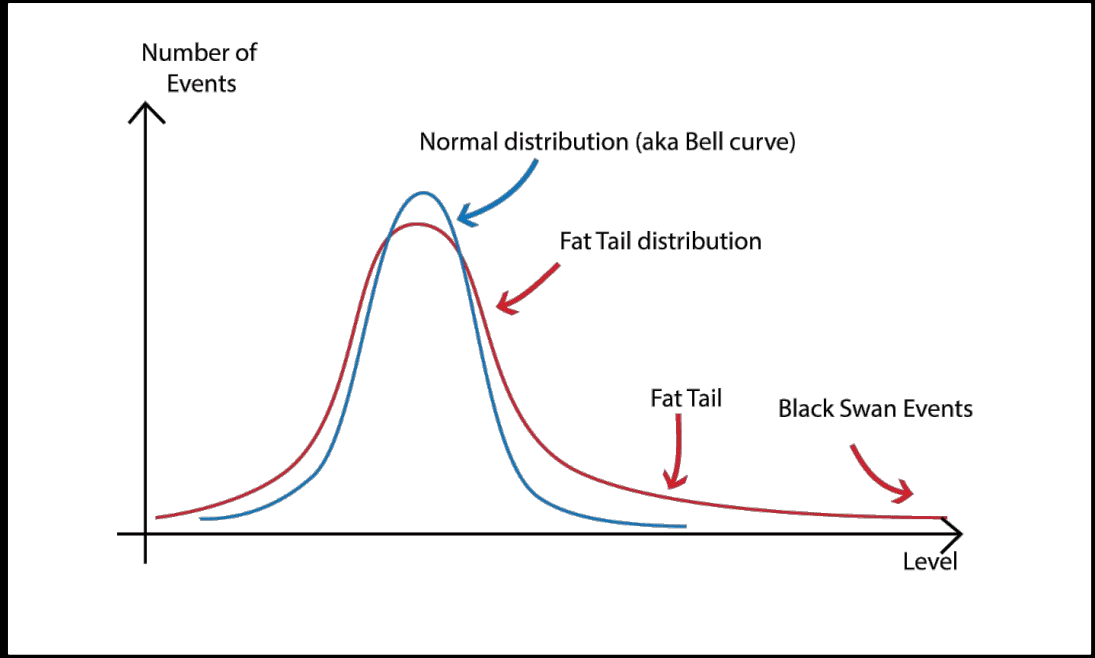
Some common risks & mitigations

Attack Type	Description	Risk	Mitigation
Phishing & Social Engineering	Deceptive emails or messages designed to steal credentials or sensitive data.	Compromised accounts, financial loss, or data breaches.	Train employees to recognize phishing attempts and use email filtering tools. Don’t click on anything you aren’t expecting.
Ransomware	Malicious software that encrypts files and demands payment for decryption.	Loss of access to critical systems and data, costly ransom payments.	Regularly back up data, update software, and use antivirus tools (Windows Defender is great place to start).
Man-in-the-Middle	Attackers intercept communication between two parties to steal or alter data.	Stolen login credentials, financial fraud, or exposure of sensitive communications.	Use encrypted connections (e.g., HTTPS, VPNs) especially over public WIFI

Really bad outcomes are really uncommon.

Cyber incidents that shut down your business are “Black Swan” events (i.e., very unlikely but still possible)

Often it is hard to justify the cost to mitigate these long tail outcomes, but things like cyber insurance can help protect your downside



Cyber Incident Exercise

Ransomware Response Exercise

What We're Doing:

- Simulating a ransomware attack at a marina to experience decision-making under pressure.
- Volunteers will take on different roles to explore how these incidents unfold and learn best practices.

Your Goals:

- Work together to minimize disruption to operations.
- Decide how to respond to the attacker while protecting your business.

Remember:

- There's no "perfect" solution.
- The exercise is about exploring risks, strategies, and trade-offs.

Roles in the Scenario

Marina Owner:
- High-level decision-maker responsible for overall strategy and financial choices.

Marina Manager:
- On-the-ground operator ensuring continuity of customer service and operations.

Customer:
- A frustrated customer needing to close their account during the attack.

Cyber Insurance Agent (Lori):
- Provides clarity on the insurance policy and financial recovery options.

Management Software Representative (Joe):
- Offers technical support for your management platform.

Local Authorities:
- Supports the community with criminal issues.

Cybercriminal:
- Puts pressure on the marina to pay the ransom, escalating the threat if ignored.

The Marina Manager starts their morning, preparing for a busy holiday weekend.

When they log into the office computer, a message appears:

"Your files have been encrypted. Pay $25,000 in Bitcoin within 48 hours, or your data will be permanently deleted."

Local systems are locked, and operations are disrupted. What will you do?

The Marina Manager receives a text from a customer:

"Hi, I'll be up at the office in a few minutes to close my account before heading out."

Do you feel ready to handle this customer?

What do you want to do next?

Suddenly, the Marina Owner receives an unexpected call. It's from the cybercriminal.

“You’re taking too long. If you don’t pay the ransom within the next hour, your systems will be locked forever”

(The criminal hangs up abruptly before the Owner can respond.)

What actions do you think you need to take now?

Debrief

Any questions?

Cyber Risk Management for Marinas

November 2024
Docks Expo

PRESENTATORS:
Lori Sousa - Sea Land Insurance Corp.
Joe Revier - Slipify

SEA LAND INSURANCE CORP

slipify better marina software

Any questions?