RETAIL & HOSPITALITY ISAC

Creating an Organizational Culture of Information Sharing and Transparency

Cyber crime is big business — it is now more profitable than the global trade of all major illegal drugs combined. With cyber threats constantly evolving, one of the best ways to reduce risk is collaboration and information sharing within the cybersecurity community.

Why is sharing important in cybersecurity?

- Cybersecurity is still a relatively new industry. Sharing best practices helps everyone in this field that is innovating on a daily basis.
- Criminals are collaborating so we need to collaborate to stop them.
- Sharing with the cyber community can help fill in the blanks when you may have data but don't fully understand how it fits into the larger puzzle.

How is sharing protected under the law?

- The Cybersecurity Information Sharing Act (CISA) provides businesses with legal protections for sharing threat intelligence, monitoring systems for cyber issues (e.g., employee monitoring), and defending systems against cyber threats.

CISA protections and considerations

- CISA allows for sharing between and among private sector and state local, and federal government agencies.
- CISA permits businesses to exchange cyber threat indicators and defensive measures for cybersecurity purposes subject to a few restrictions:
  - » Applies to sharing and receiving information from private sector
  - » CISA defines private entity to contemplate ISACs, ISAOs, and cybersecurity services providers
- CISA protections apply to both informal sharing and more formal arrangements (e.g. through an ISAC)
- CISA does not seek to restrict sharing relationships
- CISA does not mandate sharing of information
- CISA does not create a duty to share cybersecurity information or act based on the receipt of information.
- CISA requires you to remove personal information from an indicator that is not directly related to a cyber threat.
- CISA requires businesses that are sharing or receiving indicators to use security controls to protect against unauthorized access.

Creating buy-in for sharing

- **Educate key stakeholders:** Executives, legal, and business units do not have a cybersecurity background but are critical partners, particularly in incident response after a security breach. Educating these team members on cybersecurity terminology and the structure of the cyber team will make it easier for all to understand the need for information sharing and how to talk about a cybersecurity breach should it occur.

- **Be specific about what to share:** Legal teams in particular may be predisposed to be skeptical about information sharing and start from "no" if they do not understand what it is that cybersecurity teams want to share. Being specific about what will be shared and how sharing will be facilitated can help launch a productive conversation.

- **Use a template:** Create a template that guides which type of information will be shared. The template can illustrate that personally identifiable information or other confidential data will not be included.

- **Provide the benefits**: Executives, legal teams, and other business stakeholders may do a risk assessment on sharing to consider how it could impact the company's brand reputation, or create risk in the event of a lawsuit. Cybersecurity teams should make known the benefits of information sharing and that there is an upside to offset potential risk.

- **Use transparency to build trust**: Particularly after a breach, an organization may be nervous about sharing. But incident response can provide an opportunity to control the narrative and educate your customers, shareholders, and the general public about the steps your company is taking to fix the problem and mitigate risk going forward.