Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Healthcare organizations face significant supply chain cybersecurity risk management challenges, according to new survey

New Ponemon Institute research finds significant capability and budget gaps between large and small enterprises, and that organizations of all sizes still struggle with the basics

Washington, DC – January 10, 2023 - A new survey shows that more than 400 healthcare organizations face critical challenges in managing supply chain cyber risk across the healthcare industry and significant opportunities to adopt foundational supply chain risk management practices. "***The State of Supply Chain Risk in Healthcare***" research report, which was conducted by the Ponemon Institute on behalf of the Health Sector Coordinating Council (HSCC) Cybersecurity Working Group, found that significant capability and budget gaps between large and small enterprises remain, and that organizations of all sizes still struggle with the basics, such as visibility into supplier inventory, linking supply chain risk to patient impact, and integrating enterprise supply chain management with procurement and contracting functions.

Key insights from the survey include:

- **Organizations of all sizes still struggle with the basics.** Creating a full inventory of an organization's suppliers is a necessary step to effectively assessing and mitigating supplier risk. However, fewer than 20% of survey respondents have a complete inventory of their suppliers, with smaller organizations being three times more likely to have no inventory at all. Furthermore, almost half of organizations (46%) only focus their supply chain risk management programs on new suppliers onboarded since their programs began, potentially leaving a significant 'blind-spot' to the risk posed by their pre-existing supplier base.

- **Significant opportunities exist to widen the risk lens and better integrate with procurement.** 35% of health sector organizations do not evaluate supplier risks tied to patient outcomes. Smaller organizations are twice as likely to have this gap vs. larger organizations. Also, 41% of organizations consider their supplier cyber risk programs to be integrated with the procurement and contracting teams within their organizations. Smaller organizations are only half as likely as large organizations to adopt this best practice.

- **Smaller organizations face resourcing challenges.** There is a significant discrepancy in the budgetary resources available to larger vs. smaller organizations. In fact, 57% of smaller organizations have annual supply chain risk management budgets of $500,000 or less. By comparison, 51% of large organizations have annual budgets between $1M and $5M. The recent policy options paper released by Senate Select Committee on Intelligence Chairman Mark R. Warner (D-VA), "Cybersecurity is Patient Safety," outlined current cybersecurity threats facing health care providers and systems, and noted that smaller organizations may not currently have the resources or technical expertise to participate in information sharing organizations.

"This survey shows that healthcare organizations of all sizes still face an uphill battle to effectively manage cyber risk across the supply chain function, with smaller organizations still facing critical gaps in the resources and budget available to them," said Greg Garcia, HSCC Executive Director of its Cyber Security Working Group.

"The healthcare supply chain team is under an increasing amount of pressure to move quickly while managing a multitude of risks during the procurement process," Ed Gaudet, CEO and Founder of Censinet and HSCC Supply Chain Cybersecurity Task Group Member. "As cyberattacks like ransomware become more sophisticated, this survey hammers home the urgent need for automation and actionable risk insights to help supply chain leaders effectively manage inventory, cyber risk, fraud, safety, and supplier redundancy."

The survey reinforces the need for healthcare enterprises to adopt the National Institute of Standards and Technology's Cyber Security Framework supply chain management practices that the HSCC Cybersecurity Working Group tailored for the health sector in a resource known as HIC-SCRiM, the Health Industry Cybersecurity Supply Chain Risk Management Guide, a toolkit for small to mid-sized healthcare institutions to implement and sustain a supply chain cybersecurity risk management program. Since its original release in October 2019, the HIC-SCRiM guide has become one of the HSCC's flag-ship products, accessed by more than 10,000 individuals. It provides actionable guidance and practical tools to help organizations of limited scale or resources to manage the cybersecurity risks they face through their dependencies within the health system supply chain. While primarily written for small and medium sized organizations, the guide also makes a call to action for large healthcare organizations, associations and consultancies to raise awareness and encourage adoption across the sector.

The toolkit structure follows the supply chain requirements within the NIST Cyber Security Framework (CSF). The first release of HIC-SCRiM provided concrete guidance on three of the five NIST CSF supply chain requirements covering process as well as practical tools such as contractual language and risk assessment templates. This second release completes the five NIST CSF requirements by covering adherence to contractual terms and testing response and recovery in case of supplier cybersecurity incidents.

To learn more about the research with Dr. Larry Ponemon, register for our webinar scheduled for January 30, 2023, at 12:00 p.m. ET, go to:
https://h-isac.zoom.us/meeting/register/tZYudOupqj0sGNPrlojSjHuDswUYFrTS5LI9

To access and download a copy of ***The State of Supply Chain Risk in Healthcare***" research report, go to:
https://healthsectorcouncil.org/wp-content/uploads/2023/01/HCC-Report-Final-1.pdf

To access and download a copy of the HIC-SCRiM, go to https://HealthSectorCouncil.org/HIC-SCRiM-v2.

More….

The HSCC Cybersecurity Working Group has published 14 best practices and guidance documents since 2019, including:

- Operational Continuity Cyber Incident (OCCI)
- Medtech Vulnerability Communications Toolkit (MVCT)
- Model Contract-Language for Medtech Cybersecurity (MC2)
- Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT)
- Health Industry Cybersecurity Supply Chain Risk Management Guide – Version 2 (HIC-SCRiM-v2)
- Health Industry Cybersecurity Return to Work Guidance (HIC-ReWork)
- Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)
- Health Industry Cybersecurity Protection of Innovation Capital (HIC-PIC)
- Health Industry Cybersecurity Information Sharing Best Practices
- Management Checklist for Teleworking Surge During COVID-19 Response
- Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO)
- Health Industry Cybersecurity Workforce Development Guide (HC-WorkDev)
- Health Industry Cybersecurity Practices (HICP)
- Medical Device Joint Security Plan (JSP)

About the Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group (JCWG). The HSCC is an industry-driven public-private partnership of health companies and providers developing collaborative solutions to mitigate threats to critical healthcare infrastructure. It is one of 16 critical infrastructure sectors organized to partner with the government under Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience. The HSCC Joint Cybersecurity Working Group (JCWG) includes more than 370 medical device and health IT companies, direct patient care entities, plans and payers, labs, blood and pharmaceutical companies, and several government partners. The JCWG industry chair is Erik Decker, Vice President and Chief Information Security Officer for Intermountain Healthcare.

For more information: Greg Garcia, HSCC Cybersecurity Working Group Executive Director:

Greg.Garcia@HealthSectorCouncil.org or visit us online at https://healthsectorcouncil.org

###