“A must-read for any individual or organization looking to stay one step ahead of high-tech threats – and one step ahead of the curve.”
—Greg Kahn, President & CEO, Internet of Things Consortium

CYBERSECURITY

The Expert Guide™

Defending Against Disruption and Maintaining Computer Security During Times of Digital Transformation

SCOTT STEINBERG

BESTSELLING AUTHOR OF MAKE CHANGE WORK FOR YOU™

How to Promote Cybersecurity Awareness Across Your Business

Security isn't just a technical challenge for today's organization. It's also a cultural one. Given that any digital defense is only as effective as the people behind it, promoting best practices around online and high-tech interactions is crucial. That's why the best IT security strategies start with keeping cyber awareness top of mind.

Implement Formal Policies, Procedures, and Guidelines

- Define and clearly articulate cyber security policies surrounding the use of hardware devices, software, information, and high-tech exchanges of all kinds, including when and how it's appropriate to interact and communicate online.
- Establish role-based guidelines for each team, including what specifically individual members need to know about IT security, online safety/privacy, and how to comport themselves using digital channels.
- Build a formal security handbook – online, print, or PDF – that codifies these principles and guidelines, and share it with your staff.
- Provide managers with step-by-step guides to the actions that they should take with regards to getting new hires up to speed on cybersecurity, providing existing employees with continuing education, and addressing when workers depart the organization.
- Assign staffers clear security-related roles and responsibilities, including which specific teams and individuals have the authority to make decisions in the event that cyber threats are detected, and which tasks that each is empowered to pursue in support of addressing high-tech concerns.

Equip Staff with Up-to-Date Training and Instruction

- Provide employees with access to educational, training, and certification programs that promote knowledge of and hands-on experience dealing with cyber threats. Follow it up with ongoing coverage and correspondence of emerging security issues every 90 to 180 days.
- Refresh workers' knowledge of industry best practices and standards every six months, and offer access to additional sources of instruction and self-guided learning should they wish to explore these topics further.
- Implement and provide employees with internal communications channels – e.g. team chat programs or online forums – where they can discuss and share additional insights, or provide questions and feedback to their peers.
- Supplement linear sources of education such as books, training guides, and online videos with interactive exercises and team-based activities that test staffers' skills and ability to problem-solve in real-time.
- Should employees make errors or oversights as they proceed through the learning process, use these opportunities to provide constructive feedback on how to correct mistakes, and instruction into how the consequences of these choices could impact the organization's operations.

Implement Real-World Scenario Training and Feedback

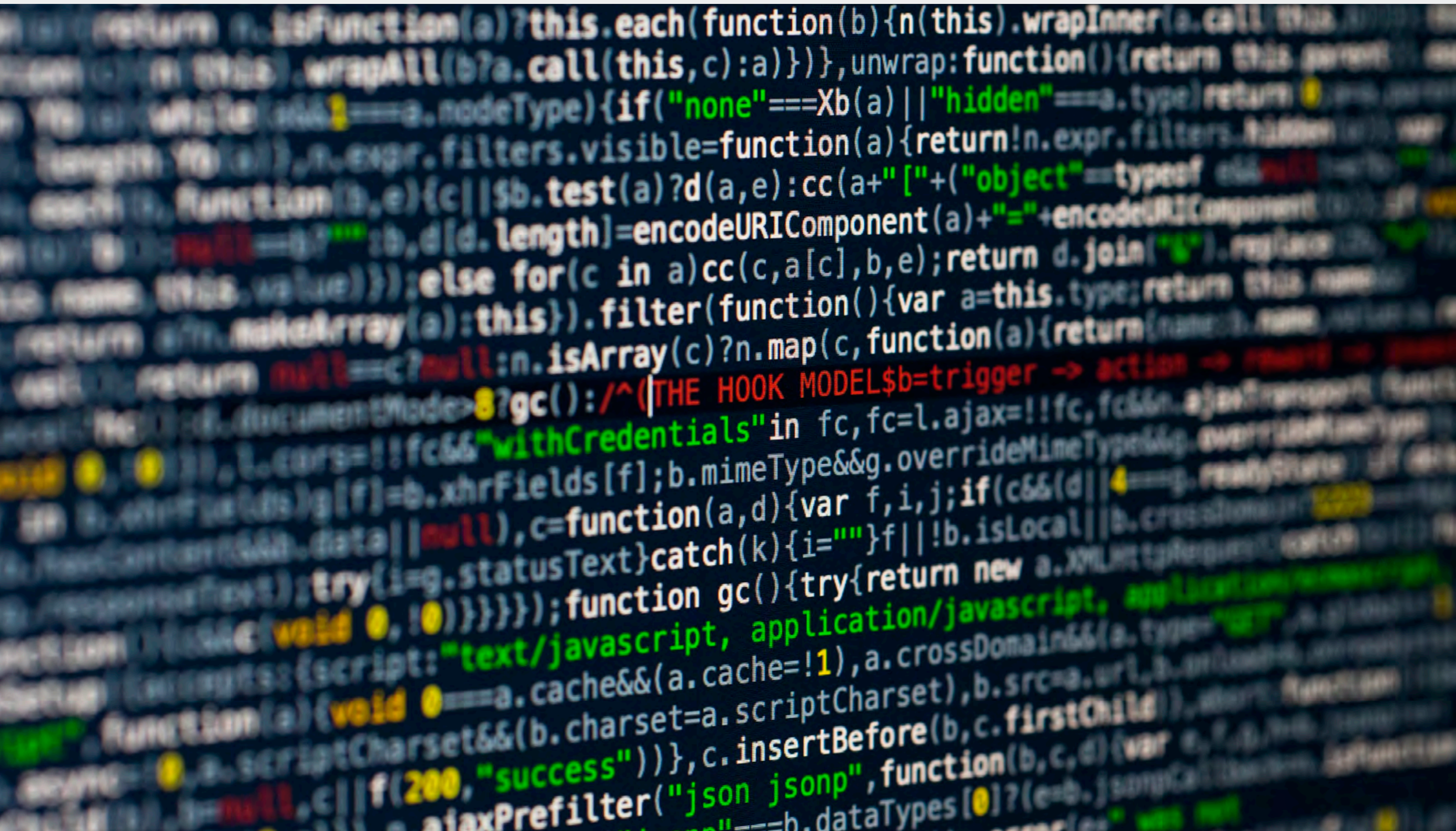
- Transform day-to-day cybersecurity challenges and concerns – e.g. encounters with phishing, social engineering, or business email compromise – into realistic, simulated real-world scenarios that employees can work through to grow their skills and expertise.
- Offer instructional feedback as workers tackle these challenges, helping them think through potential courses of action, consider the potential risks and rewards associated with every choice, and determine the optimal means of addressing each encounter.
- Give staff the autonomy to puzzle their own way through scenarios, and chances to collaborate and work as a team, encouraging them to share ideas and input all the way. In tandem, make a point to remind them that it's OK to make mistakes – but important not to make the same mistake twice.
- Quiz employees on what they've learned, review the results of these sessions, and discuss where strategies should be revisited and updated to be more effective.
- Gather the insights gleaned from these exercises and share them with other areas of the organization.

Promote Knowledge and Awareness Amongst Your Staff

- Articulate why cybersecurity matters at every turn: When someone joins the team, provide one-on-one and group training sessions; when incidents occur, review what happened with staffers; and when conducting annual planning, schedule instructional sessions to occur at regular intervals throughout the year.
- Plan and schedule regular content marketing and employee engagement campaigns that also promote knowledge and awareness of cybersecurity topics and trends amongst your staff.
- Reach out and address employees on a routine basis – e.g. weekly or monthly – about rising topics of IT concern, and encourage them to embrace a mindset wherein they constantly work to Identify (recognize), Measure (prioritize), Monitor (review), and Control (limit) prospective risks.
- Maintain online resources and forums when employees can turn to stay current on cyber threats and IT industry trends.
- Create a communications plan and workflow for dealing with IT security incidents, outline the disaster response process, and familiarize it amongst your teams.
- Avoid laying blame when security issues arise, and use these incidents to provide employees with refresher courses and opportunities to analyze what went wrong so they can better address them in the future.

Institute Comprehensive Reporting and Analysis

- Identify the key person(s) accountable for cyber security within each of your firm's departments, and circulate their contact info amongst staffers. Do the same for each of your partners and vendors. Also provide information on emergency and off-hours contacts.
- Implement official communications channels – e.g. tip lines, online forums, or emergency email accounts – through which employees can document and report any cyber security events or incidents. These platforms should include mechanisms that allows information about potential security threats to flow freely between employees and IT decision makers.
- Educate workers on whom to call upon or reach out to if a cyber event happens, especially if systems, websites, or services need to be quarantined or shut down on short notice.
- Standardize threat reports and updates to help employees quickly share information using time-saving templates.
- Define threat severity levels, and articulate to workers under what circumstances they should escalate concerns higher up official channels.



Implementing High-Tech Safety at Work

The more often you encourage employees to exercise healthy cybersecurity skills, the more they'll become a routine habit. Here's how to get started.

- **Take accountability** – Teach every employee that cyber security begins with them, and to speak up and say something if they spot concerns.
- **Provide ongoing education** – Keep workers current on cyber security best practices and standards, and refresh this training every three to six months.
- **Cultivate healthy skepticism** – Encourage staff to maintain a reasonable sense of concern, and institute a multi-step verification process that encourages employees to double-check every important query or request with their peers.
- **Simulate emergencies** – Test workers' ability to respond to threats in real-time by regularly simulating real-world challenges and popular news events, allowing them to exercise their skills in practical, problem-solving challenges.
- **Be supportive** – Encourage employees to report suspicious activity by removing the stigma associated with being fooled, and share their insights as incidents occur so that the organization can learn from them.
- **Offer constructive criticism** – Rather than punish workers for making mistakes, use them as teachable moments to provide practical feedback and reinforce cyber security best practices.
- **Encourage interactivity** – Provide staff with running access to events, educational opportunities, and team-building activities that promote the cultivation and development of cybersecurity skills.

10 Questions to Ask Yourself and Third-Party Vendors

- How are you implementing and maintaining cybersecurity best practices?
- What type of IT security training and instruction are you providing your employees – and how often?
- How is data classified and handled by your organization?
- Are you constantly updating and testing your IT safeguards?
- What security standards are internal workers and partners being held to?
- How are your employees and your vendors being vetted and verified?
- What security policies are in place in the event of network compromise or breach?
- How often and where is data being backed up?
- In addition to digital defenses, what physical safeguards are in place to protect sensitive information?
- What provisions exist for recovering network access or info if it is stolen or compromised?

INNOVATIVE
HEALTHCARE SPEAKERS

(406) 586-8775 or
Info@InnovativeHealthcareSpeakers.com
for more information.