CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

CYBERSECURITY CULTURE CHEAT SHEET

① Security belongs to everyone

A Sustainable Security Culture requires that everyone in the organization is committed. Everyone must act with security at top-of-mind.
Security belongs to everyone, from the executive staff to the lobby ambassadors. Everyone owns a piece of the company's security solution and security culture. A misstep by anyone can bring disaster.

② Focus on Awareness

Security awareness is the process of teaching your entire team the basic lessons about security..You must set the level of each person's ability to judge threats before asking them to understand the depth of the threats. Awareness is an ongoing activity, so never pass up a good crisis.Grow your security culture with these teachable moments, using them as an example for how the team can get better..

③ Reward Actions

When someone goes through the mandatory security awareness program and completes it successfully, give them something substantial. A simple $100 cash reward is a huge motivator for people, and will cause them to remember the security lesson that provided the money. The return on investment on preventing just a single data breach greatly outweighs the $100 spent.

Educate ④

Cyber security is a critical aspect of business. While many people think of cyberattacks as being some hacker forcing their way through a security wall or exploiting a piece of software, many cyber security breaches occur when employees inadvertently allow an attacker. In many cases, the employee is unaware of their part in the attack. The best way to keep your company's data safe is to teach your staff to avoid potentially risky behaviors and to know what to do in case of an attack.

Be Consistent ⑤

Cybersecurity is a marathon, not a sprint. Training and information should be shared on a consistent basis. Monthly emails or videos are a great way to keep the training going. Occasional training, including informal trainings before shifts, can keep the awareness up without requiring you to subject your employees to long, tedious seminars about cyber security.
Additionally, keeping a line of communication open is important. Having a phone number that people can call with questions or if there's an incident can reduce problems and improve response time.

Continue reading on next page >

CYBERSECURITY CULTURE CHEAT SHEET

CRAIG PETERSØN.COM

(CONTINUED)

6 Add Fun

Many associate security with boring training or it being so restrictive that they can't get their work done. To cement a sustainable security culture, build-in fun.

Consider using gamification to build fun and engagement into all aspects of security in your business.

For instance, a game of security trivia using a different security category each time. Or find hackers in the movies one month and security news in another. These are examples of how to bring fun and engagement into the process.

7 Positive Change

The good news is that building a simple security culture can positively change how the organization approaches security. With the right process and attitude, you'll get there.

Build Your Community 8

Community is the backbone of a sustainable security culture. It helps build multiple connections between people across the organization. A Security Community assists in bringing everyone together against the common problem, and eliminates an "us versus them" mentality.

An effective security community is achieved by understanding the different security interest levels within the organization: advocates, the security aware, and sponsors. It can manifest as one-on-one mentoring, weekly or monthly meetings to discuss the latest security issues, and involves everyone at every level within the organization..

Software Development Lifecycle 9

The processes and activities that your organization agrees to perform for each software or system release are known as a Secure development lifecycle (SDL.) It includes things like security requirements, threat modeling, and security testing activities -- a sustainable security culture in action!

Provide opportunities for team members to grow into a dedicated security role through advancement. If you say security is important, prove it by providing growth potential for those with a passion for security.

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH