SECURITY READINESS WORKSHOP

A Methodical Approach to Understanding and Improving Your Organization's Security Posture

BENEFITS

VISION: Gain better vision into your organization's entire security environment

RISK: Identify how to measure, evaluation and manage risk, while isolating specific gaps in the current processes

CONSENSUS: Build consensus of security issues and steps needed among executives and key stakeholders across the organization

ACTION: Receive a prioritized and actionable roadmap for security initiative

AN INTELLIGENT APPROACH

Protecting your business-critical assets and information has become a top priority for organizations regardless of size and industry. Most organizations have implemented security process and tools to address potential threats. However, many organizations have yet to create cohesive strategy and actionable plan centered around the organization's business goals. These organizations aspire to implement and adopt security measures, but are not sure where to start, where to focus their priorities, or how to overcome institutional challenges.

Organizations need security strategies that are closely aligned with business goals. Our comprehensive Security Readiness Assessment is intended to provide you the information required to determine the security risks in your environment, current processes, and the strategy and steps to improve your security posture to meet business goals. You'll gain a better understanding of these three key areas:

Heuristics: Heuristics can be described as what you "see" is happening on the network. They provide vision into everything that is happening in the security environment. This tends to be the first item discussed as it cascades down to all other subjects. With a clearer view of the heuristics, you will have a better understanding of the gaps in vision, and the processes around what to do if/when you see suspicious activity.

Habits: The actions, abilities, and mindset of a person in the organization. This also includes the policies, technology, and event vision to either contain bad habits or enforce good ones.

Hygiene: The quality of data and processes and how often they are updated. The hygiene section commonly discusses points around data quality in monitoring systems and user activity, and policies and procedures around the usage of data.

THE WORKSHOP METHODOLOGY + FOCAL AREAS

The **Security Readiness Workshop** uses our proven engagement methodology to ensure a high-value result. A highly collaborative 3-5 hour whiteboard session with key executives and stakeholders takes a holistic review of the entire security environment of your organization. Our security experts review objectives, identify the current status and provide a plan of action.

Process Review: Identify what processes have been created, which ones are missing, and the current process follow through with focus on "Does it exist," "How current is the policy," and "Is it being followed?"

Monitoring & Logging: Review current monitoring process, what technology is being monitored, what are "best practices" in place and what are future plans.

Technology Review: Takes a deeper dive at what technology is currently in place and whether it is being used to help mitigate corporate risk. The review begins with the intrusion model of "main targets" and expands from there.

Prioritization: Together the group prioritizes the remediation for each gap found based on value for the cost, difficulty in the department and fit into the business plan.

WHAT TO EXPECT

The complete gap assessment and prioritization roadmap is presented onsite or via teleconference; the duration of the entire engagement is generally 1-2 weeks.

WHY InterVision?

InterVision has secured the networks of hundreds of organizations including financial institutions, government agencies, technology companies, and multinational corporations. This includes designing and implementing information security solutions in the areas of VPNs, firewalls, authentication, encryption, intrusion detection, email, and remote access. Our engineers are cross-trained in all areas critical to IT environments including networking, enterprise applications, cloud, wireless, storage and virtualization. They have experience with complex security environments and understand current best practices.

Learn more about how InterVision can help you understand and improve your organization's security posture:
*Visit **www.intervision.com** or contact your InterVision Account Manager.*