

# ① Driving Cybersecurity Policies



Security policy is the statement of responsible decision makers about the protection mechanism of a company crucial physical and information assets.

**MAKE SURE YOU HAVE:**

- Provided for Independent, Comprehensive and Effective Audit Coverage of IT Controls
- Ensured system of internal controls is operating effectively
- Identified Security Procedures and Policies
- Implemented Personal and Physical Security Procedures and Policies
- Password Security Procedures and Policies
- Data Privacy Procedures and Policies
- Business Continuity and Disaster Recovery Procedures and Policies
- Cybersecurity Training Procedures and Policies
- Compliance Review Procedures and Policies



**CRAIG PETERSON**

AMERICA'S LEADING SECURITY COACH

# CEO CYBERSECURITY RESPONSIBILITIES CHEAT SHEET

## ② Understanding Risks



Risk is commonly defined as  
 $\text{Threat} \times \text{Vulnerability} = \text{Consequence}$

When applied to cybersecurity—businesses face unique risks as a result of using interconnected technological systems combined with the Human Element.

- Evaluating and Managing your business' specific cyber risks:
  - Human error
  - General threats
  - Access control threats
  - Refusal threats
  - Legal and regulatory threats
- Inform Board about current cyber risks and business impact to company
  - Ensure full understanding, including consequences
- All cyber discussions should classify risks as:
  - Avoidable
  - Acceptable
  - Can Mitigate
  - Transfer liability to insurance

## Understanding Risks (cont.) ②

- Ensure there is a plan to address each identified risk
- Set expectation for establishing an enterprise-wide risk management framework with adequate staffing and budget
- Ensure that cyber risks are part of existing risk management and governance framework
- Understand the legal and regulatory implications of cyber risks as they apply to your company and its circumstances
- Ensure that conversations about cyber risks are given regular and adequate time on agendas for corporate meetings
- Hold Management and Board Accountable for IT Risks
  - Identification
  - Measuring
  - Mitigation
- Ensure there is a specific process for notifying executive leadership
- Have Crisis Management Team organized and ready to respond

# CEO CYBERSECURITY RESPONSIBILITIES CHEAT SHEET

MAINSTREAM.NET

(CONTINUED)

## ③ CyberSecurity



Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises cybersecurity and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems.

- Understand both the types, and the number of cyber incidents detected weekly in your business
- Make sure all incidents are prioritized based on impact to your company and your data assets
- Avoid burn-out of your cybersecurity team by using integrated security systems
- Ensure that your program complies with industry standards and best practices
- Promote effective IT governance
- Review and approve your IT strategic plan. Ensure it aligns with your overall business strategy
- Don't rely completely on compliance, but implement industry standards and best practices
- Provide oversight and review
- Oversee, review, and receive updates on
  - IT projects
  - IT budgets
  - IT priorities
  - Overall IT performance
- Oversee the adequacy and allocation of IT resources for both funding and personnel
- Oversee process for approving third-party providers offering services to your business



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We are not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, we make no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. We make no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.



# CRAIG PETERSON

AMERICA'S LEADING SECURITY COACH