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

CEO CYBERSECURITY RESPONSIBILITIES CHEAT SHEET

② Understanding Risks

Risk is commonly defined as Threat X Vulnerability = 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

Continue reading on next page >

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

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH