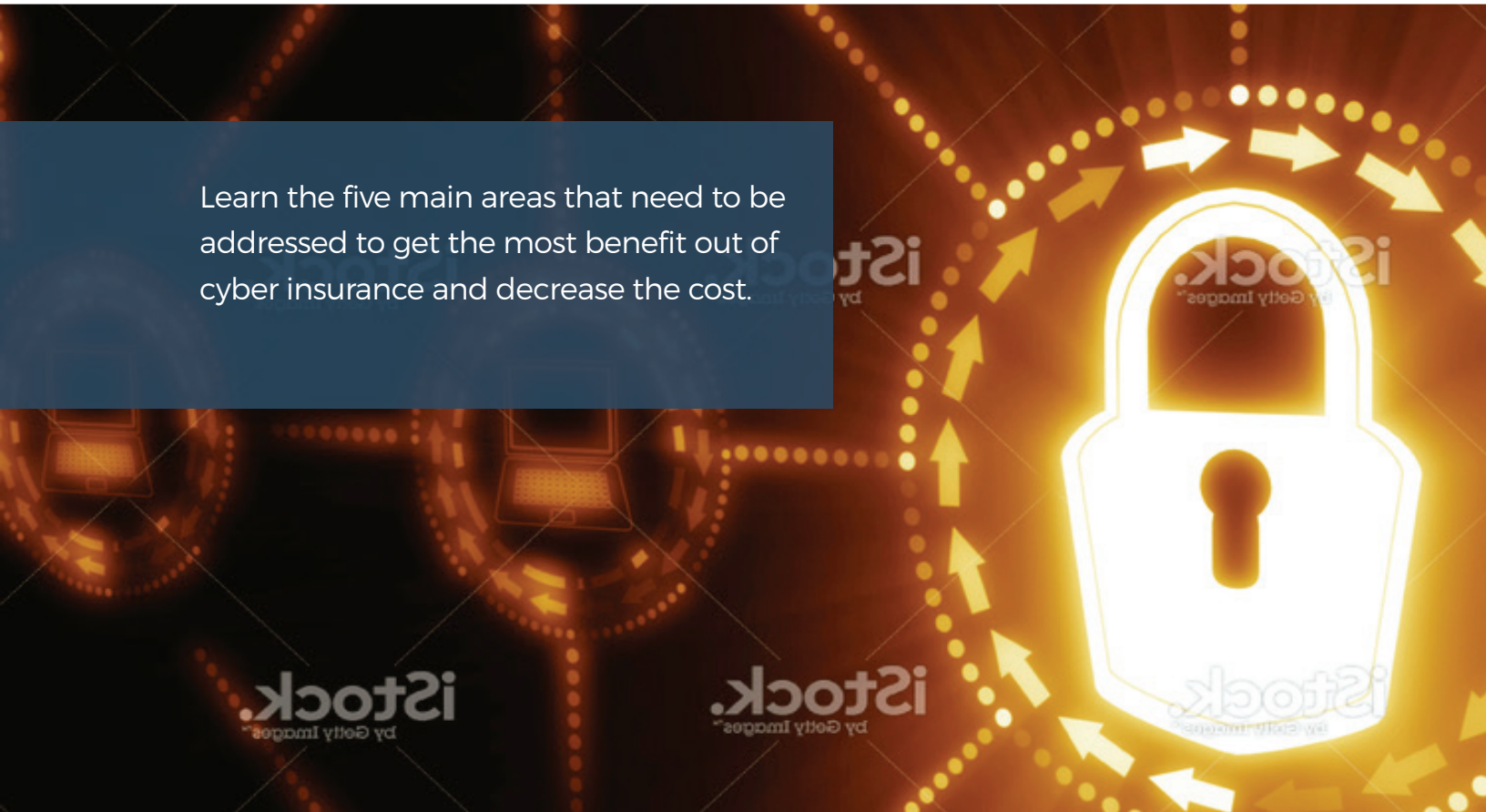
Cask

PERSPECTIVE BY CASK EXPERTS

MAXIMIZE THE VALUE

OF YOUR INVESTMENT WITH CYBER INSURANCE

Learn the five main areas that need to be addressed to get the most benefit out of cyber insurance and decrease the cost.



Your Cyber Data is Increasingly at Risk – **and So Is the Reputation of Your Organization**

"I've had a lot of worries in my life, most of which never happened." MARK TWAIN

DAILY THREATS ARE HERE TO STAY

There were almost 61,000 cyber attacks and security breaches across the entire federal government in 2014

DECEMBER 14, 2014
CNN

While many worries never actually occur, the undeniable fact is that the risk of cyber events such as computer hacks, data loss, and the resulting potential damage to an organization's image are very real. And the possibility of a negative cyber event is becoming more common every day.

One way to help ameliorate that risk is with insurance. While relatively new, cyber insurance is quickly becoming an essential component of risk management in every organization. It can cover the costs of:

- Data breach response
- Forensic investigations
- Customer notifications
- Call center response
- Credit monitoring
- Data restoration
- Public relations' costs
- Legal fees
- Regulatory costs such as fines
- Liability costs to both the organization and third parties.

Just as a responsible head of household obtains life insurance, a responsible organization now needs to integrate Cyber Insurance as part of risk management or Business Resilience efforts. When applying for life insurance, "risky lifestyle habits" such as smoking or sky diving may

result in increased premiums or outright denial of coverage. The same is true for Cyber Insurance. So when applying for Cyber Insurance, what are the equivalent "cyber habits" that may result in increased or decreased premiums or denial of coverage?

In determining what cyber habits may need to change to increase Cyber Resiliency and facilitate a decrease in Cyber Insurance premiums, the following five steps will ensure that an organization's people, processes, and technology will be accurately evaluated, fully engaged, and equitably balanced.

Just as a responsible head of household obtains life insurance, a responsible organization now needs to integrate Cyber Insurance

Five Steps to Maximizing Cyber Insurance Coverage

Implement a Business Cyber Strategy

One key component in potentially decreasing the cost for Cyber Insurance is for an organization to implement a cyber-business strategy that is flexible enough to adapt to rapidly evolving threats. Ensuring appropriate governance, proper stakeholder management, valid policies, and compliance checks all contribute to a solid cyber strategy.

To go a little deeper, when it comes to governance and policies, both must be clearly defined, well communicated, and centrally managed. Stakeholders should understand their roles and engage regularly. Compliance with legal, regulatory, and contractual requirements must be monitored, measured, and documented. An easy way to remember this is through the values of:

✓ EDUCATE ✓ ESTABLISH ✓ ENFORCE

An organization must educate the workforce, clearly establish policies and procedures, and must enforce the policies and procedures through periodic assessments.

Document Technology Design and Architecture

Understanding and documenting the design and architecture of the technology that supports your organization, and ensuring that this design and architecture compliments the organization's business cyber strategy is another key component in potentially decreasing insurance costs. Key things to consider when laying the groundwork for a robust Technology Design and Architecture are:

- The interaction of personnel with the organization's technology
- Architecture
- Management of third parties and the supply chain
- A solid business continuity plan
- Appropriate use of technology such as endpoint security and cryptography

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT, SED DO EIUSMOD TEMPOR INCIDIDUNT UT LABORE ET DOLORE MAGNA ALIQUA. UT ENIM AD MINIM.

Third parties that interact with the organization's environment need to first be identified and then managed to ensure that no threat is posed. A Business Continuity Plan and process must be in place, be kept current, and tested annually at a minimum. Finally, technologies such as Endpoint Security and Cryptography must be integrated and managed to provide maximum benefit.

Transition the Strategy Into Operations

A third key component in potentially decreasing Cyber Insurance costs is for an organization to transition the strategy into operations. As part of this transition, there are several areas which must be addressed:

- Inventory and management of assets and asset configurations
- Managing appropriate access to data
- Management of data in transit and data at rest
- Proper disposal of data
- Testing and training

These activities provide measurable results that need to harmonize within organization strategy, architecture, and operations.

Critical assets must be properly identified, controlled, and managed. Both assets and data must receive appropriate attention so proper handling, access, and protection is ensured.

Data transportation, storage, and removable media procedures must be established and adhered to. Change management procedures must be developed and implemented. The operational environment and its components must be regularly tested in accordance with standard frameworks and methodologies. Training concerning the cyber environment must be conducted for all personnel. This training must then be continually updated and utilized by all team members. Documentation of management procedures must be in place, reviewed, maintained, and updated. Finally, the organization's data retention and disposal plan must be in accordance with best practices, and in compliance with appropriate laws, statutes, and regulations.

DAILY THREATS ARE HERE TO STAY

The state of Michigan is spending millions every year fending off up to 187,000 daily online attacks on states records.

MARCH 7, 2013
CBS NEWS CHANNEL 3

Execute the Plan in Operations

Operations is where the plan developed from the organizational strategy and the architectural design is put into effect. Optimal execution includes implementation and management of access controls, administration of network security, supervision of physical and operations security, and the execution of the incident management plan. These efforts, among others, when implemented correctly and operated efficiently, reduce risk and decrease the costs of transferring risk to a cyber-insurer.

Having the correct controls in place will deter, detect, and correct internal and external threats. Proper access controls allow for regular monitoring and safeguarding of information. Proper security management and incident management may minimize disruptions to an organization.

Create a Continual Improvement Plan

Even in a smoothly operating organization, the constant transformation of the threat, business, and technology environments introduce friction that may take the organization off track. Strategy drives a cycle of design, transition, and operations, and a culture of continual improvement must be integrated in the organization to ensure continued success. Key components of a Continual Improvement Plan are:

- Audits and reviews
- Assessment of implemented controls
- Benchmarking
- Improvements in process
- Business continuity rehearsals

Continual improvement that contributes to maintaining the smooth operation of an organization may result in decreasing Cyber Insurance costs.

Audits and assessments of controls and setting benchmarks can help identify where an organization might benefit from change. They can identify the state that an organization is currently in, and can serve as the starting point for plotting a course to take the organization to where it needs to be. Testing the activation of an organization's Business Continuity Plan can ensure that it works efficiently when it is needed. Finally, a remediation plan can be put in place for areas that require improvement.

Taking the **Next Step**

The areas discussed only scratch the surface of this complex issue.

An in depth analysis of an organization needs to be conducted to ensure solid footing when an organization is considering Cyber Insurance and wants the lowest possible premium. These preparatory steps may decrease premiums, but more importantly, considering each point carefully will give greater awareness of areas of potential risk within the organization.

What we've walked through is the AXELOS RESILIA™ best practice, a framework that delivers a balanced approach in the prevention, detection and correction of cyber-attacks, emphasizing the importance of and providing guidance for, an effective balance between people, processes, and technology while delivering organizational resilience. As one of the first five AXELOS Consulting Partners globally, Cask applies best practice frameworks to ensure the entire organization plays a role in business resiliency to include the prevention, detection and response to security incidents.

In a 2012 online Forbes Magazine article there are no fewer than 13 types of insurance that even a small organization should carry, including data breach insurance. If you are ready for your organization to explore Cyber Insurance, Cask, as a certified AXELOS Consulting Partner (ACP), can help you ask the correct questions and apply the AXELOS RESILIA™ framework to obtain the information you need to move forward and strategically implement effective solutions to make your organization Business Resilient.

DAILY THREATS ARE HERE TO STAY

In January 2014, hackers stole personal information from an estimated 110 million accounts

DECEMBER 31, 2014
NEWSWEEK

ABOUT US

Cask provides acquisition, program, and technology management consulting. operational excellence using TBM principals and best practices, including Portfolio Management, IT Planning & Budgeting, and Cost Transparency.

Technology Business Management

- TBM Readiness & Startup
- Cost Transparency
- IT Planning/Budget
- Investment Optimization
- Decision Support
- IT Financial Management

Portfolio and Project Management

- PMO Implementation, Operationalization, and Enhancement
- PPM Coaching
- PPM Solution Design
- PPM sub-disciplines (APM, SPM, PLM, etc.)

Program Support Services

- Acquisition Management
- Program, Project, & Schedule Management
- Cost Estimation & Financial Planning
- Systems Engineering, Logistics, Technology, and IT SMEs

Service Management & Operations

- Maturity Assessments
- Service Management Strategy & Roadmaps
- Service Portfolio & Catalog Design
- ITIL Best Practices
- Rapid Process Improvement Workshops

Cyber Security & Resiliency

- Cyber Security and IA Assessments
- Cyber Resiliency Management
- Information and Security Planning
- Governance, Risk & Compliance

Business Transformation Services

- Organizational Change Management
- Business Process Management
- Measurement Systems & Reporting
- Performance Management
- Execution Support

Cask Delivers Business And Technology Advisory And Consulting Services To Help **Our Customers Achieve Success**.

CONTACT US

For more information about how Cask's TBM services can help with IT business management, please contact us:

Kate Ehrle
540-370-0905
Kate.Ehrle@Caskllc.com

Dave Honaker
202-465-4216
Dave.Honaker@Caskllc.com